WatchGuard® Firebox System Configuration Guide

WatchGuard System Manager 8.3
WFS Appliance Software 7.4.1

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2006 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*. A copy of this book is automatically installed into a subfolder of the installation directory called Documentation. You can also find it online at:
http://www.watchguard.com/help/documentation/

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Management Software: WSM 8.3
Appliance Software: WFS 7.4.1
Document Version: 7.4.1-352-2673-001

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:
www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:
U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.

Contents

CHAPTER 1 Getting Started with WFS Appliance Software 3
What is Appliance Software? 3
Installing WFS appliance software 3
Using WFS appliance software tools 4
About Incoming and Outgoing Traffic 4
CHAPTER 2 Using the Firebox System Manager 5
Starting the Firebox System Manager 5
Using the Security Traffic Display 6
Monitoring status information 7
Selecting the middle of the star 7
Firebox System Manager Indicators 7
Traffic and load indicators 8
Firebox and VPN tunnel status 8
Monitoring Firebox Traffic 10
Changing the Polling Rate and the maximum number of log messages 10
Using color for log messages 12
Copying log messages 12
Learning more about deny and allow messages 12
Doing Basic Tasks with Firebox System Manager 13
Rebooting the Firebox 13
Reboot IPSec 13
Flushing the ARP cache 13
Connecting to a Firebox 14
Viewing Bandwidth Usage 14
Viewing Number of Connections by Service 15
Viewing Information About Firebox Status 16
Status Report 16
Authentication 20
Blocked Sites 20

Security Services 21
HostWatch 21
HostWatch 22
Connecting HostWatch to a Firebox 22
Controlling the HostWatch window 22
Changing HostWatch view properties 23
CHAPTER 3 Designing Your Network Architecture 27
Adding a firewall to your network 27
Selecting a firewall configuration mode 28
Routed configuration 29
Drop-in configuration 30
Adding secondary networks to your configuration 31
Dynamic IP support on the external interface 31
CHAPTER 4 Basic Firebox Configuration 33
Opening a Configuration File 33
Opening a configuration from the Firebox 34
Opening a configuration from a local hard disk 34
Saving a Configuration File 34
Saving a configuration to the Firebox 35
Saving a configuration to the management station 36
Changing the Firebox passphrases 36
Setting the Firebox Model 37
Setting the Time Zone 37
Setting a Firebox Friendly Name 38
CHAPTER 5 Using Services to Create a Security Policy 39
Packet Filters and Proxies 39
Services and the Policy Manager 39
Selecting Services for your Security Policy 40
Incoming and outgoing services 40
Incoming service guidelines 40
Outgoing service guidelines 41
Adding and Configuring Services 41
Changing the Policy Manager View 42
Service Parameters to Configure 42
Adding a service 44
Making a new service 44
Adding more than one service of the same type 46
Deleting a service 47
Configuring Service Properties 47
Opening the Service Properties dialog box 47
Adding service properties 48
Adding addresses or users to service properties 48
Working with wg_icons 49
Customizing logging and notification 49

Service Precedence 50
CHAPTER 6 Configuring the Network Interfaces 53
Making a New Configuration File 53
Setting the IP Addresses of Firebox Interfaces 54
Setting addresses in drop-in mode 54
Using proxy ARP 55
Setting the addresses in routed mode 57
Configuring the external interface 57
Setting the external interface for DHCP 58
Setting the external interface for PPPoE 58
Using a static DHCP or static PPPoE address 59
Adding external IP aliases 59
Adding Secondary Networks 60
Adding WINS and DNS Server Addresses 61
Configuring the Firebox as a DHCP Server 61
Adding a subnet 62
Changing a subnet 63
Removing a subnet 63
Adding Basic Services to Policy Manager 63
Configuring Routes 65
Adding a network route 65
Adding a host route 66
Firebox interface speed and duplex 66
CHAPTER 7 Configuring Proxied Services 69
Protocol Anomaly Detection 69
Customizing Logging and Notification for Proxies 70
Configuring an SMTP Proxy Service 70
Configuring Incoming SMTP Proxy 71
Enabling protocol anomaly detection for SMTP 75
Configuring the Outgoing SMTP Proxy 76
Configuring An FTP Proxy Service 78
Enabling protocol anomaly detection for FTP 79
Selecting an HTTP Service 79
Adding a proxy service for HTTP 80
Configuring a caching proxy server 81
Configuring the DNS Proxy Service 82
Adding the DNS Proxy Service 82
Enabling protocol anomaly detection for DNS 83
DNS file descriptor limit 83
CHAPTER 8 Configuring Network Address Translation 85
Dynamic NAT 86
Using Simple Dynamic NAT 86
Enabling simple dynamic NAT 86
Adding simple dynamic NAT entries 87

Reordering simple dynamic NAT entries 87
Specifying simple dynamic NAT exceptions 87
Using Service-Based Dynamic NAT 88
Enabling service-based dynamic NAT 88
Configuring service-based dynamic NAT 88
Configuring Service-Based Static NAT 89
Setting static NAT for a service 89
Using 1-to-1 NAT 90
Proxies and NAT 92
CHAPTER 9 Creating Aliases and Implementing Authentication 93
Using Aliases 93
Adding an alias 94
How User Authentication Works 95
Using external authentication 96
Enabling remote authentication 96
Authenticating from optional networks 96
Using authentication through a gateway Firebox to another Firebox 96
Authentication Server Types 96
Defining Firebox Users and Groups 97
Configuring Windows NT Server Authentication 99
Configuring RADIUS Server Authentication 99
Configuring CRYPTOCard Server Authentication 101
Configuring SecurID Authentication 102
Configuring a Policy with User Authentication 102
CHAPTER 10 Intrusion Detection and Prevention 105
Default Packet Handling 105
Blocking spoofing attacks 106
Blocking port space and address space attacks 106
Stopping IP options attacks 107
Stopping SYN Flood attacks 107
Changing SYN flood settings 107
Unhandled packets 108
Blocking Sites 108
Blocking a site permanently 108
Creating exceptions to the Blocked Sites list 109
Changing the auto-block duration 110
Logging and notification for blocked sites 110
Blocking Ports 110
Avoiding problems with approved users 111
Blocking a port permanently 111
Auto-blocking sites that try to use blocked ports 112
Logging and notification for blocked ports 112
Blocking Sites Temporarily with Service Settings 112
Configuring a service to temporarily block sites 112

Viewing the Blocked Sites list 113
Integrating Intrusion Detection 113
Using the fbidsmate tool 114
CHAPTER 11 Connecting with Out-of-Band Management 115
Connecting a Firebox with OOB Management 115
Enabling the Management Station 115
Preparing a Windows NT management station for OOB 115
Preparing a Windows 2000 management station for OOB 116
Preparing a Windows XP management station for OOB 116
Configuring the Firebox for OOB 117
Establishing an OOB Connection 118
CHAPTER 12 Configuring BOVPN with Manual IPSec 121
Configuration Checklist 121
Configuring a Gateway 122
Making a Tunnel with Manual Security 125
Making a Tunnel with Dynamic Key Negotiation 127
Making a Routing Policy 128
Configuring routing policies for proxies over VPN tunnels 130
Changing IPSec policy order 130
Configuring multiple policies per tunnel 131
Configuring services for BOVPN with IPSec 131
Enabling the BOVPN Upgrade 131
CHAPTER 13 Configuring IPSec Tunnels 133
Management Server 133
WatchGuard Management Server Passphrases 134
Setting Up the Management Server 135
Adding Devices 136
Updating a device's settings 136
Configuring a Firebox as a Managed Firebox Client (Dynamic Devices only) 137
Adding Policy Templates 138
Get the latest templates from a device 138
Make a new policy template 138
Adding resources to a policy template 139
Adding Security Templates 139
Making Tunnels Between Devices 139
Drag-and-drop tunnel procedure 140
Using the Add VPN Wizard without drag-and-drop 140
Editing a Tunnel 141
Removing Tunnels and Devices 141
Removing a tunnel 141
Removing a device 141
CHAPTER 14 Configuring RUVPN with PPTP 143
Configuration Checklist 143

Encryption levels 143
Configuring WINS and DNS Servers 144
Adding New Users to Authentication Groups 145
Configuring Services to Allow RUVPN Traffic 146
By individual service 146
Using the Any service 146
Activating RUVPN with PPTP 147
Enabling Extended Authentication 148
Entering IP Addresses for RUVPN Sessions 148
Configuring Debugging Options 149
Preparing the Client Computers 149
Installing MSDUN and Service Packs 149
Creating and Connecting a PPTP RUVPN on Windows XP 150
Creating and Connecting a PPTP RUVPN on Windows 2000 150
Running RUVPN and Accessing the Internet 151
Making Outbound PPTP Connections From Behind a Firebox 151
CHAPTER 15 Controlling Web Site Access with WebBlocker 155
Getting Started with WebBlocker 155
Add an HTTP Service 155
Configuring the WebBlocker Service 155
Activating WebBlocker 156
Allowing WebBlocker server bypass 156
Configuring the WebBlocker Message 156
Scheduling operational and non-operational hours 157
Setting privileges 158
Setting privileges 158
Creating WebBlocker exceptions 158
Managing the WebBlocker Server 159
Installing Multiple WebBlocker Servers 160
CHAPTER 16 Maintaining Connectivity with High Availability 161
The High Availability Failover Process 161
Installing High Availability 163
Connecting Fireboxes in a High Availability Pair 164
If you do not have a Firebox installed 164
If you have one Firebox installed now. 164
Configuring High Availability 165
Configuring High Availability with the wizard 165
Configuring High Availability manually 166
Testing the failover process 168
Indentifying the active and standby Fireboxes. 168
Backing up an HA configuration 168
CHAPTER 17 Protecting Users with Gateway AntiVirus for E-mail™ 169
About Virus Signatures 169

Gateway AntiVirus for E-mail Procedures 170
Installing Gateway AntiVirus for E-mail 170
Enabling Gateway AntiVirus for E-mail 171
Getting Gateway AntiVirus for E-mail Status and Updates 172
Seeing Gateway AntiVirus for E-mail status 172
Updating Gateway AntiVirus for E-mail signatures 172
Updating the antivirus engine 173
Clear Gateway AntiVirus for E-mail statistics 173
Configuring Gateway AntiVirus for E-mail System Settings 173
Configure Gateway AntiVirus for E-mail 173
Configuring Gateway AntiVirus for E-mail in the SMTP Proxy 174
Add an SMTP Proxy with Gateway AntiVirus for E-mail 174
Configure Gateway AntiVirus for E-mail for an existing SMTP Proxy 176
Using Gateway AntiVirus for E-mail with More Than One Proxy 177
Gateway AntiVirus for E-mail Headers 177
Monitoring Gateway AntiVirus for E-mail Activity 177
CHAPTER 18 SpamScreen 179
SpamScreen Options 179
Customizing SpamScreen using Multiple Proxies 180
Installing SpamScreen 180
Starting SpamScreen 181
Configuring How the Firebox Handles Spam 181
About SpamScreen headers and tags 181
Tagging messages 183
Denying spam 183
Allowing spam 184
Logging spam 184
Determining How SpamScreen Identifies Spam 184
Configuring RBL/DNS Servers 185
Adding RBL Servers 186
Configuring Spam Rules 186
Adding spam rules 187
Restoring default rules 188
Importing rules 188
Defining spam threshold weight 188
Configuring Exceptions to the Spam List 189
Blocking addresses not on the spam list 190
Monitoring SpamScreen Activity 190
Viewing message header notifications 190
Interpreting log messages 191

PART I Introduction to WFS Appliance Software

CHAPTER 1

Getting Started with WFS Appliance Software

When you purchase a WatchGuard® Firebox®, you receive management software and a hardware appliance. The management software includes the WatchGuard System Manager, Management Server, Log Server, and tools to configure the Firebox as well as to monitor its status.

What is Appliance Software?

Appliance software is a software program or operating system which is permanently stored on your hardware. You can use the management station to save appliance software on your Firebox® X. The Firebox uses the appliance software in combination with the configuration file to operate. When you upgrade your Firebox device, you write a new version of the appliance software to its memory.

There are now two types of appliance software available to WatchGuard customers:

- WFS — This is the default appliance software on Firebox III and Firebox X Core devices. This is the standard version of the appliance software successfully used by WatchGuard customers since 1998. WatchGuard System Manager v8.0 includes WFS v7.4.
- Fireware — This is the default appliance software on Firebox X Peak devices. If you have a Firebox X Core, you can purchase a Fireware upgrade. This software offers customers advanced features which are optimized for more complex networks. It includes these advanced features:
  - Signature-based IDP
  - Gateway AntiVirus for E-Mail
  - Advanced networking options including QoS, dynamic routing, and support for multiple WANs

Installing WFS appliance software

When you install the WatchGuard System Manager, it automatically installs the software tools you need to configure and manage a Firebox III or Firebox X device with WFS appliance software. These include:

- Firebox System Manager for WFS
- Policy Manager for WFS
- HostWatch for WFS

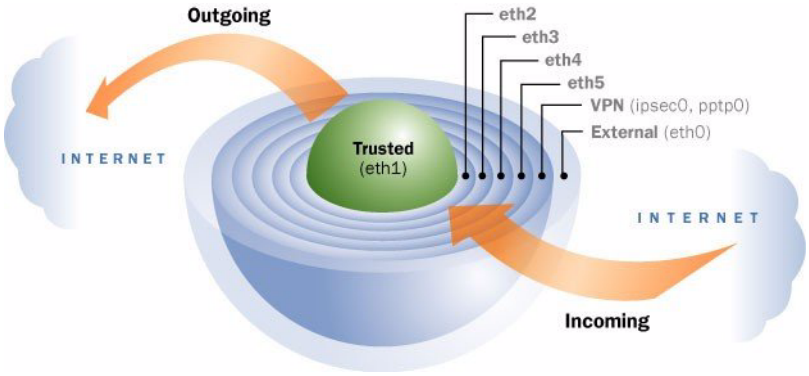
Using WFS appliance software tools

When you add a device to the WatchGuard System Manager Devices tab, the application identifies which appliance software the Firebox uses. If you select the Firebox and then click an application icon on the toolbar, it automatically starts the correct management tool.

For example, add a Firebox X700 to the Devices tab using the instructions found in the WatchGuard System Manager User Guide. Select the Firebox X700. Click the Policy Manager icon on the WSM toolbar. Policy Manager for WFS starts and opens the configuration file.

About Incoming and Outgoing Traffic

Network traffic is classified as either incoming traffic or outgoing traffic. The figure below shows the direction of network traffic as it goes through all the possible Firebox interfaces. Incoming traffic goes to the center. Outgoing traffic goes away from the center.



Note

This figure shows a Firebox® X and the 3-Port Upgrade to enable three more Ethernet ports. The traffic flow and trust relations between the different Firebox interfaces apply if you have the upgrade or not.

The distance to the center determines the level of security and the level of trust. WatchGuard recommends that you decrease the number of incoming connections as you move to the center. The networks are near the center because you use more restrictive rules for those networks. We call these networks trusted. The farther you move from the center, the less secure and the less trusted the networks become as you increase the number of incoming connections.

The external interface is the source of traffic that has no security (eth0). It is usually the Internet.

The source of traffic with the most security is the trusted interface (eth1), the center of the figure.

All network traffic that goes out from your trusted network is outgoing traffic. The destination network makes no difference. All the traffic that comes into your trusted network is incoming traffic. The source in the organization makes no difference.

All the traffic that comes from the external interface is incoming traffic. The destination network behind your Firebox makes no difference. All the traffic to the external interface is outgoing traffic. Again, the source in the organization makes no difference.

CHAPTER 2

Using the Firebox System Manager

WatchGuard® Firebox® System Manager for WFS lets you monitor the status of a single Firebox device. You can also use the Firebox System Manager to monitor real-time traffic through the firewall.

Starting the Firebox System Manager

You start the Firebox System Manager from the WatchGuard System Manager. The WatchGuard System Manager automatically identifies if a Firebox uses WFS appliance software or Fireware appliance software and starts the correct version of the Firebox System Manager.

1 Open the WatchGuard System Manager.
For more information on the WatchGuard System Manager, see the *WatchGuard System Manager User Guide*.

2 Select **File** > **Connect to** > **Device**.

Or
Click the Connect to Device icon on the WatchGuard System Manager toolbar. The icon is shown at left.
The Connect to Firebox dialog box appears.

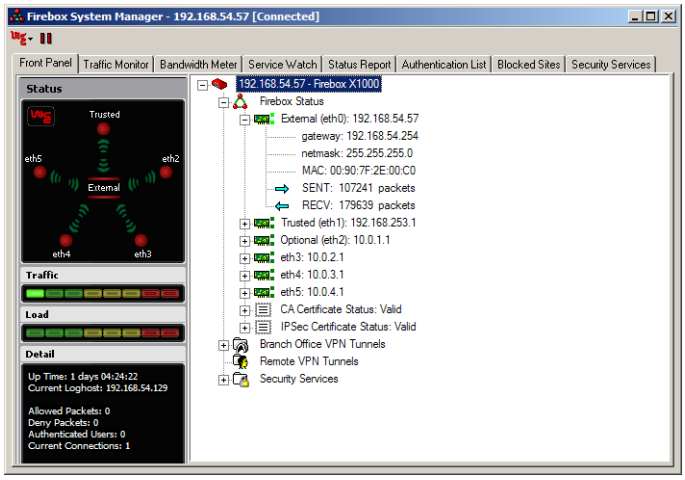
3 Select a Firebox from the **Firebox** drop-down list.
You can also type the IP address or name of the Firebox. You can connect to a Firebox, or you can cancel the Connect to Firebox dialog box and connect to a Firebox at a different time.

4 In the **Passphrase** text box, type the Firebox status (read-only) passphrase.

5 Click **OK**.
The Firebox appears in the Device tab of the WatchGuard System Manager.

6 Select **Tools** > **Firebox System Manager**.

Or
Click the Firebox System Manager icon on the WatchGuard System Manager toolbar. The icon is shown at left.
The Front Panel tab of the Firebox System Manager appears.

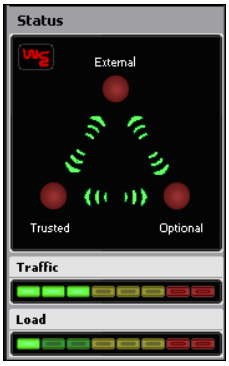


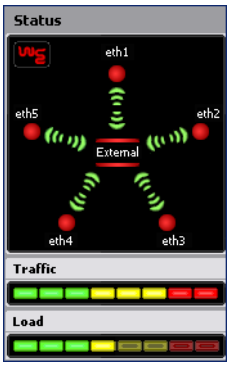
Note

Do not use the configuration (read-write) passphrase to monitor the Firebox. You can not make more than one read-write connection at the same time. When you connect to the Firebox with Firebox System Manager, the passphrase you enter is used again to get the configuration file from the Firebox and open it in Policy Manager. If you connect with the read-write passphrase, you can not open Policy Manager, because that is a second read-write connection.

Using the Security Traffic Display

The Firebox System Manager initially shows a group of indicator lights to show the direction and volume of the traffic between the Firebox® interfaces. The display can be a triangle (below left) for Fireboxes with three interfaces, or the display can be a star (below right) for Fireboxes with six interfaces.





To change the display, right-click it and select **Triangle display** or **Star display**. A Firebox with three interfaces can not use the Star display.

Monitoring status information

The WatchGuard logo in the top, left corner of the Star display or Triangle display shows if the Firebox is connected. If the WatchGuard logo is bright, the Firebox is connected. If the graphic is dim, it is not connected.

The points of the star and triangle show the traffic that flows through the interfaces. Each point shows incoming and outgoing connections with different arrows. When traffic flows between the two interfaces, the arrows show in the direction of the traffic.

In the star figure, the location where the points come together can show one of two conditions:

- Red (deny) — The Firebox is denying a connection on that interface.
- Green (allow) — There is traffic between this interface and a different interface (but not the center) on the star. When there is traffic between this interface to the center, the point between these interfaces shows as green arrows.

In the triangle, the network traffic shows in the points of the triangle. The points show only the idle and deny conditions.

Selecting the middle of the star

If you use the star figure, you can customize which interface appears in its center. The default star figure shows the external interface in the center. When you put a different interface in the center, you can see all traffic between that interface and the other interfaces. Click the interface name or its point. The interface then moves to the center of the star. All the other interfaces move in a clockwise direction.

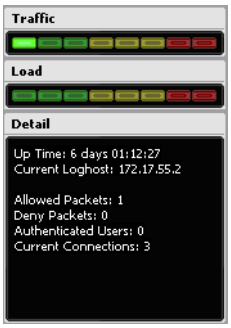
Firebox System Manager Indicators

The top part of the window immediately below the title bar contains buttons to do basic operations and to start Firebox System Manager tools.

Icon	Function
	Open the main menu for Firebox System Manager. This is also referred to as the Main Menu button.
	Stop the connection to the Firebox. This icon only appears when you are connected to a Firebox. If you are not connected, the icon shows as a green triangle. Click this triangle to connect to the Firebox.

Traffic and load indicators

Below the security traffic figure are the traffic volume indicator, processor load indicator, and basic status information.



The two bar graphs show the traffic volume and the Firebox® capacity. The amount of time the Firebox has been operational and the log host IP address are also displayed. For more information on the front panel, refer to the FAQ:

https://www.watchguard.com/support/advancedfaqs/fbhw_lights.asp

Firebox and VPN tunnel status

The section in Firebox System Manager to the right side of the front panel shows:

- The status of the Firebox.
- The branch office VPN tunnels.
- The remote user VPN tunnels.
- The Security Services status.

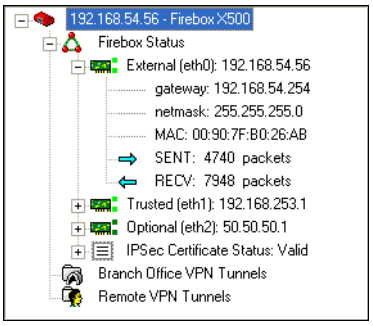
Firebox Status

Below Firebox Status, you can see:

- Status of the High Availability feature. When it has a correct configuration and is serviceable, the IP address of the standby Firebox appears. If High Availability is installed, but there is no network connection to the secondary Firebox, a message appears with the words "Not Responding."

The High Availability feature only appears if you have purchased and added a High Availability license.

- The IP address of each Firebox interface and the configuration mode of the External interface.
- Status of the CA (root) certificate and the IPSec (client) certificate. This information shows only if you have an operating Management Server.



If you expand the entries below Firebox Status, you can see:

- IP address and netmask of the default gateway.

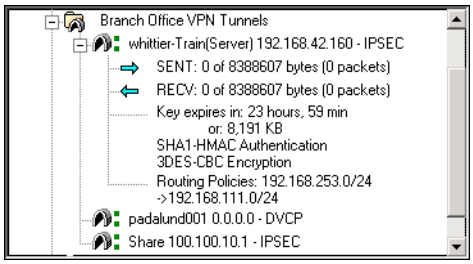
- The Media Access Control (MAC) address of each interface.
- Number of packets sent and received since the last Firebox restart.

Branch Office VPN Tunnels

Below the Firebox Status is a section on BOVPN tunnels. There are two types of BOVPN tunnels: IPSec and DVCP.

The figure below shows an expanded entry for a BOVPN tunnel. The information that shows, from the top to the bottom, is:

- The name the tunnel got when it was made, the IP address of the remote IPSec device, and the tunnel type (IPSec or DVCP).


Branch Office VPN Tunnels
whittier-Train(Server) 192.168.42.160 - IPSEC
SENT: 0 of 8388607 bytes (0 packets)
RECV: 0 of 8388607 bytes (0 packets)
Key expires in: 23 hours, 59 min
or: 8,191 KB
SHA1-HMAC Authentication
3DES-CBC Encryption
Routing Policies: 192.168.253.0/24
->192.168.111.0/24
padalund001 0.0.0.0 - DVCP
Share 100.100.10.1 - IPSEC

- The volume of data sent and received on the tunnel in bytes and packets.
- The time before the key expires and when the tunnel will start again with a new IPSec key. This appears as a time limit or as the volume of bytes. If you configure a tunnel to expire using time and volume limits, the two expiration values appear. The tunnel will start again with a new IPSec key when the limit of bytes is reached, or when the time limit is reached.
- Authentication and encryption data for the tunnel.
- Routing policies for the tunnel. (We support only one routing policy per tunnel.)

Remote VPN Tunnels

After the branch office VPN tunnels is an entry for remote VPN tunnels. This includes Mobile User VPN (with IPSec) or RUVPN (with PPTP) tunnels.

If the tunnel is Mobile User VPN, the entry shows the same information as for a Branch Office VPN. This includes the tunnel name, the destination IP address and the tunnel type. Below that is the packet information, the time for key expiration, authentication, and encryption data.

Each Mobile User VPN account you create will cause a tunnel to appear in this area. It does not matter if the MUVPN client is not connected. If Mobile User VPN uses Extended Authentication Groups, a tunnel will show for every address in the Virtual IP Address Pool. A Mobile User VPN account will display more than once if the Mobile User VPN account is configured to access more than one group of resources.

If the tunnel is RUVPN with PPTP, the Firebox System Manager shows only the quantity of sent and received packets. The volume of bytes and total time are not applicable to PPTP tunnels. A PPTP tunnel will only show when a remote user connects.

Security Services

Security Services status is for Gateway AntiVirus. For information, see the Gateway AntiVirus Guide. Gateway AntiVirus is an optional feature you can purchase.

The Security Services status shows if you have a Gateway AntiVirus license or if you do not.

Expanding and closing tree views

To expand a part of the display, click the plus sign (**+**) adjacent to the entry, or double-click the name of the entry. To close a part, click the minus sign (**–**) adjacent to the entry.

A Branch Office VPN Tunnel or a Mobile User VPN Tunnel display will have a plus sign (+) only when the tunnel construction is complete. When no plus or minus sign shows, the tunnel construction is not complete.

Red exclamation point

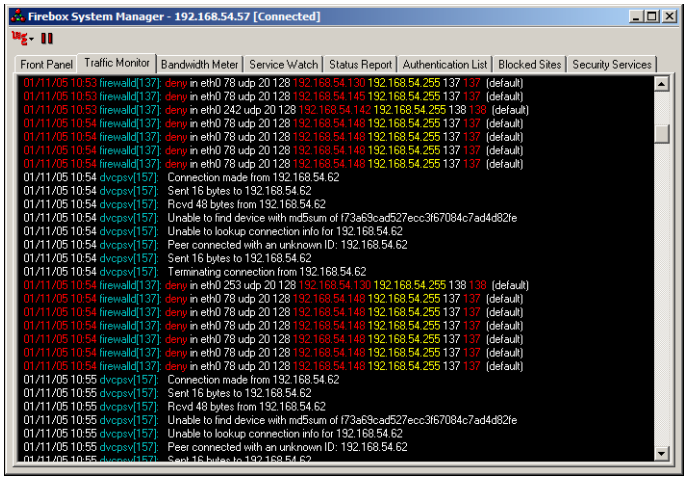
When a red exclamation point appears, it shows that something in the tree view can not send or receive traffic. For example, a red exclamation point adjacent to the Firebox entry shows that it can not send traffic to the log host or the management station. A red exclamation point adjacent to the BOVPN icon shows there is a problem with one of the VPN tunnels.

When you expand an entry that has a red exclamation point, a second exclamation point appears adjacent to the device or tunnel with the problem. Use this feature to find connection problems in your VPN network.

Monitoring Firebox Traffic

To see Firebox® log messages, click the **Traffic Monitor** tab. For more information about the messages that appear, refer to the FAQ:

https://www.watchguard.com/support/advancedfaqs/log_main.asp



Changing the Polling Rate and the maximum number of log messages

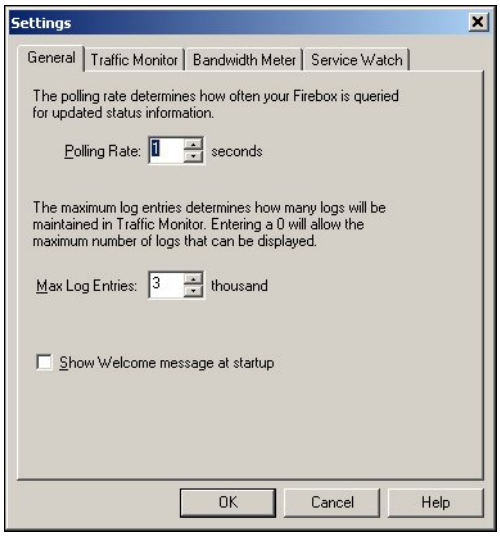
You can change the interval of time (in seconds) that Firebox System Manager gets the Firebox information and sends updates to the Front Panel and the Firebox and Tunnel Status panels. You must balance how frequently you get information and the load on the Firebox. A shorter time interval gives a more accurate display, but makes more load on the Firebox.

You can also change the maximum number of log messages that you can keep and see on the Traffic Monitor. When you get to the maximum number, the new log messages replace the first entries. A high value in this field puts a large load on your management station if you have a slow processor or a small

quantity of RAM. If it is necessary to examine a large volume of log messages, we recommend that you use the LogViewer.

You can modify the polling rate or maximum number of Traffic Monitor log entries. From the Firebox System Manager:

1 Click the **Main Menu** button. Click **Settings**.
The Settings dialog box appears. It shows the General tab.



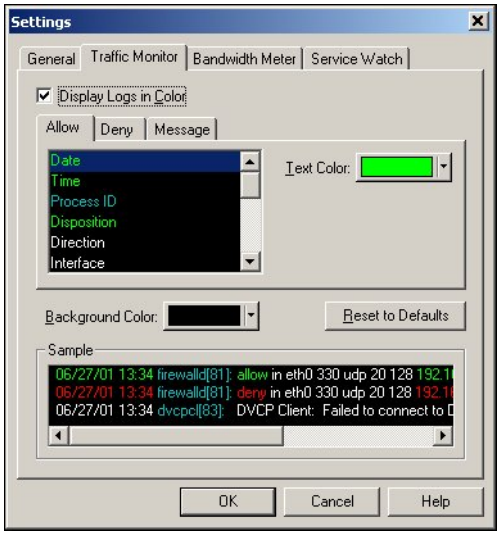
2 In the **Polling Rate** text box, type how long between queries for Firebox status information, and then click **OK**.
You can also use the value control to set the Polling Rate.

3 In the **Max Log Entries** text box, type how many log entries are maintained by the Traffic Monitor, and then click **OK**.
You can also use the value control to set the Max Log Entries. The value you type gives the number of log messages in thousands. If you type zero (0) in this field, the maximum number of log messages is set to 3,000.

Using color for log messages

You can change the color of the data components of the log messages that the Firebox sends to the Traffic Monitor. You can match a color with an information type. For example, you can set up the colors to make the log messages for denied packets red. From the Firebox System Manager:

1 Click **Main Menu** > **Settings**. Click the **Traffic Monitor** tab.



2 To enable the display of colors, select the **Display Logs in Color** check box.

3 On the **Allow**, **Deny**, or **Message** tab, click the data you want to show in a color.

4 From the **Text Color** drop-down list, select the color you want assigned to the data.
The Text Color list includes 20 colors. The information in this field appears in the new color on Traffic Monitor. You can see the color change in the sample Traffic Monitor at the bottom of the dialog box.

5 You can also select a background color for the traffic monitor. From the **Background Color** drop-down list, select the color you want for the background.
The Background Color list includes 20 colors.

6 To cancel the changes you made in this dialog box since you opened it, click **Reset to Defaults**.

Copying log messages

To make a copy of a log message and paste it in a different tool, right-click the message and select **Copy Selection.** To select a group of entries together, select the first entry, then hold the Shift key and select the last entry. To select two or more entries that are not in the same group, hold the Ctrl key while you click the entries you want. Open the other tool and paste the message.

Learning more about deny and allow messages

To learn more about a deny or allow message, you can:

- Make a copy of the source or destination IP address of a deny or allow message so you can paste it into a different software application. To copy the source IP address, right-click the message, and click **Source IP** > **Copy**. To copy the destination IP address, right-click the message, and click **Destination IP** > **Copy**.
- To ping the source or destination IP address of a deny or allow message: right-click the message, and click **Source IP** > **Ping** or **Destination IP** > **Ping**. With this command you must give the configuration passphrase.

- To use a traceroute command to a source or destination IP address of a deny or allow message: right-click the message, and click **Source IP** > **Trace Route** or **Destination IP** > **Trace Route**. With this command you must give the configuration passphrase.

Doing Basic Tasks with Firebox System Manager

The basic tasks in System Manager are:

- Reboot the Firebox
- Reboot IPSec
- Flush the ARP cache
- Connect to a Firebox®

Rebooting the Firebox

To restart the Firebox from the Firebox System Manager:

1 Click **Main Menu** > **Management** >**Reboot Firebox**.

2 In the **Passphrase** text box, type the Firebox configuration (read/write) passphrase.

3 Click **OK**.
The Firebox starts again.

You can also reboot a Firebox from the Policy Manager. From the Policy Manager click **File** > **Reboot...** Type the IP address or host name of the Firebox, and the configuration (read/write) passphrase.

Reboot IPSec

To make all IPSec VPN tunnels start again, you can reboot IPSec. You can also use this to disconnect Mobile User VPN sessions. To reboot IPSec from the Firebox System Manager:

1 Click **Main Menu** > **Management** > **Reboot IPSec**.

2 In the **Passphrase** text box, type the Firebox configuration (read/write) passphrase.

3 Click **OK**.
The IPSec procedures on the Firebox start again.

Flushing the ARP cache

The ARP cache (Address Resolution Protocol cache) on the Firebox keeps a list of the hardware addresses (also known as MAC addresses) of all the TCP/IP hosts the Firebox knows about. Before an ARP request starts, the system examines if a hardware address is in the cache. If a computer changes its IP address, an old entry in the Firebox ARP cache can cause problems for the next computer that uses the old IP address. "Old" is approximately five minutes for the ARP cache. The ARP cache clears and builds again automatically, or you can clear it manually.

From the Firebox System Manager.

1 Click **Main Menu** > **Management** > **Flush ARP Cache**.

2 In the Passphrase text box, type the Firebox configuration (read/write) passphrase.

3 Click **OK**.
This clears the ARP cache entries.

Connecting to a Firebox

When you start Firebox System Manager, you automatically connect to the Firebox selected in the Devices tab of the WatchGuard System Manager. You can connect to that Firebox or any Firebox on the network.

From Firebox System Manager:

1 Click **Main Menu** > **Connect...**
The Connect to Firebox dialog box appears.

2 From the **Firebox** drop-down list, select the Firebox you want.
You can also type the IP address or DNS name of the Firebox. When you type an IP address, type all the numbers and the dots. Do not use the TAB or arrow key.

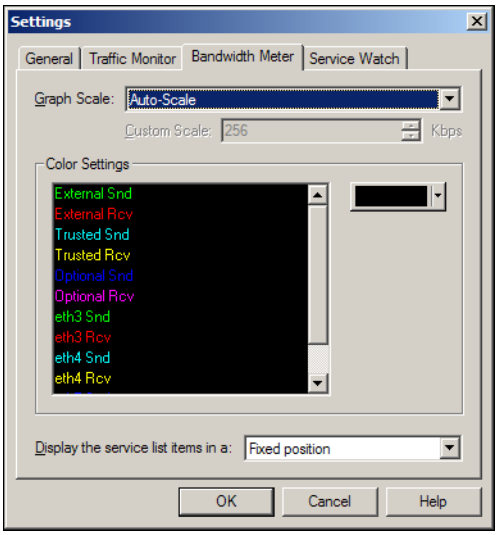
3 Type the Firebox status (read-only) passphrase. Do not use the configuration (read-write) passphrase in the **Connect to Firebox** dialog box. If you use the configuration passphrase, then you can not start the Policy Manager from the Firebox System Manager.

4 Click **OK**.
Firebox System Manager connects to the Firebox and the real-time status appears.

Viewing Bandwidth Usage

Select the **Bandwidth Meter** tab to see the available real-time bandwidth for all the Firebox® interfaces. Each interface that you see on the display has a different color. You can configure the colors that you use on this display. From the Firebox System Manager:

1 Select **Main Menu** > **Settings**. Click the **Bandwidth Meter** tab.

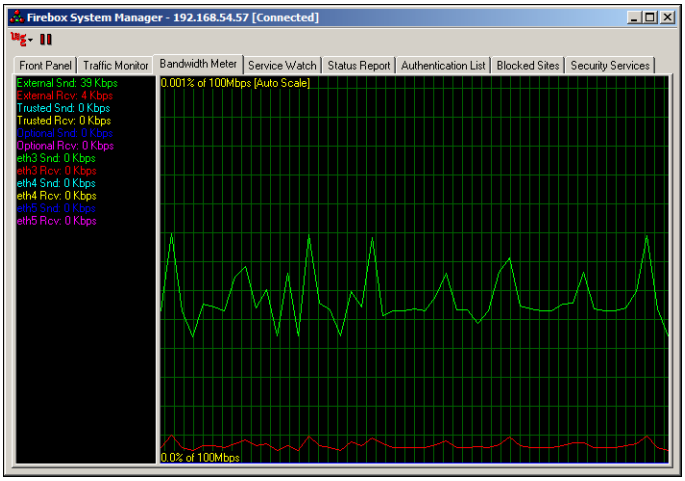


2 You can change the scale of the Bandwidth Meter graph. From the **Graph Scale** drop-down list, select the value that is the best match for the speed of your network.

3 You can also change the color of the lines in the Bandwidth Meter graph. Each line shows the traffic for one interface. In the Color Settings list, click the interface you want to change. From the Color drop-down list, select the color you want.

4 In the **Display the Service List Items in a**: drop-down list, select to keep the list items in a fixed position in the services column, or to **Align with Chart**.

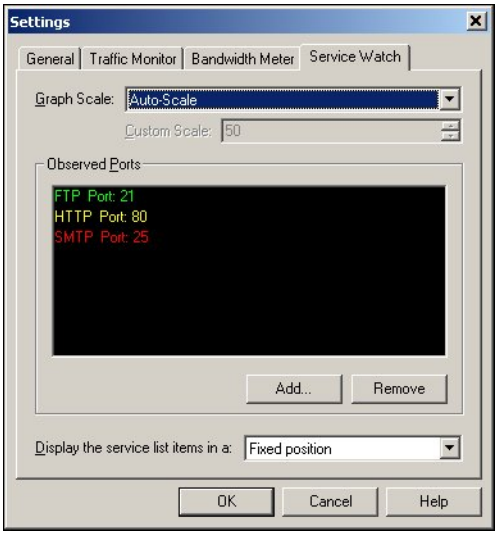
5 Click **OK** to close the Settings dialog box.
The Bandwidth Meter tab appears with the new settings.



Viewing Number of Connections by Service

The **Service Watch** tab of the Firebox System Manager makes a graph of the number of connections using a port over time. Because many well-known services use one port, you can see the connections by service using Service Watch. The Y axis shows the number of connections. The X axis shows the time. Each service that you see on the display has a different color. You can configure which services appear and their color. From the Firebox System Manager:

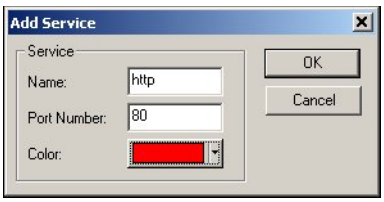
1 Click **Main Menu** > **Settings.** Click the **Service Watch** tab.



2 You can change the scale of the Service Watch tab. From the **Graph Scale** drop-down list, select the value that is the best match for the speed of your network.

Adding a service to the Service Watch tab

1 To add a service to the Service Watch tab, click **Add**.
The Add Service dialog box appears.

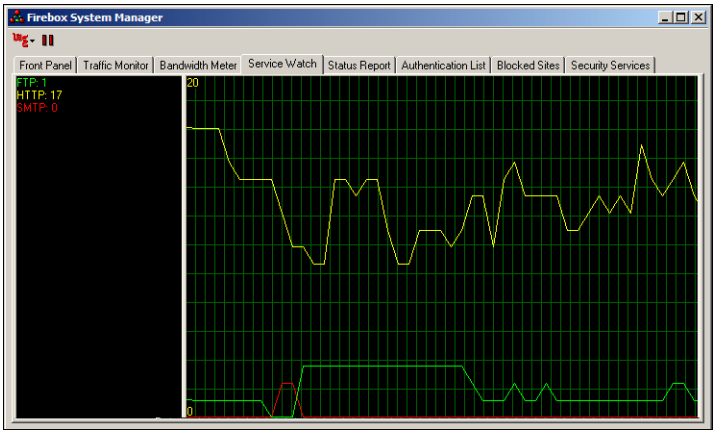


2 Type the **Name** of the service.
It is not necessary that this be the same name as the service name in the Policy Manager. This name appears only in the Service Watch graph.

3 Type the **Port Number** of the service.
This is the port that the Firebox monitors and for which it shows the traffic.

4 Use the **Color** control to select a color for the service.
We recommend that each service use a different color.

5 Click **OK** to close the Add Service dialog box. Click **OK** to close the Settings dialog box.
The Service Watch tab appears with the new settings.



Viewing Information About Firebox Status

There are four tabs that can give you information about Firebox® status and configuration: **Status Report**, **Authentication List**, **Blocked Sites**, and **Security Services** (that you see only after installing the optional Gateway AntiVirus for E-mail).

Status Report

The **Status Report** tab on Firebox System Manager gives important information about Firebox status and configuration.

Time statistics

The first section of the Status Report tells you the current time and information about how long the Firebox has been in operation.

Sample

```
Current UTC time (GMT): Sun Oct 31 19:19:35 2004

+----- Time Statistics (in GMT) ----------------------
| Statistics from Sun Oct 31 19:19:30 2004 to Sun Oct 31 19:19:35 2004
| Up since Thu Oct 28 13:44:42 2004 (3 days, 05:35)
| Last network change Thu Oct 28 13:44:41 2004
+-----------------------------------------------------
```

Version information

You can use the System Report to learn more about the management software and appliance software versions. You can also see which software components are installed on the Firebox.

Sample

```
WatchGuard, Copyright (C) 1996-2004 WGTI
Firebox Release:  sparks
Driver version:  7.4.B2248
Daemon version:  7.4.B2248
Sys_B Version:  4.61.B730
BIOS Version:  0.38

Serial Number: 203100012
Product Type: Firebox X1000
Product Options: hifn

Firebox Modular Components:
boot  0    365 7.4.B2248    8f99a151acd Sun Mar 20 17:01:34 PDT 2005
root  500  5036 7.4.B2248   43e79f4f78f Sun Mar 20 17:01:29 PDT 2005
```

Packet counts

This is the number of packets allowed, denied, and rejected between status reports. “Rejects” are packets that the Firebox denies with an ACK message.

Sample

```
Allowed:       5832
Denied:        175
Rejects:       30
```

Log hosts

The IP address of the log host. If you have more than one log host, the IP addresses of all log hosts appear in the report.

Sample

```
Log host(s): 206.148.32.16
```

Network configuration

Settings for the Firebox network interface cards. This includes: the interface name, IP addresses, and netmasks. The report also includes network route information and IP aliases.

Sample

```
Network Configuration:
lo local 127.0.0.1 network 127.0.0.0 netmask 255.0.0.0
eth0 local 192.168.2.2 network 192.168.2.0 netmask 255.255.255.0 outside
eth1 local 192.168.253.1 network 192.168.253.0 netmask 255.255.255.0
eth2 local 10.0.1.1 network 10.0.1.0 netmask 255.255.255.0
eth3 local 10.0.2.1 network 10.0.2.0 netmask 255.255.255.0
eth4 local 10.0.3.1 network 10.0.3.0 netmask 255.255.255.0
eth5 local 10.0.4.1 network 10.0.4.0 netmask 255.255.255.0
```

Blocked Sites list

This section of the Status Report shows all the IP addresses that you manually add to the Blocked Sites list. To see the temporarily blocked IP addresses, open the Firebox System Manager **Blocked Sites** tab.

Sample

```
Blocked list
network 10.0.0.0/8 permanent
network 172.16.0.0/12 permanent
network 192.168.0.0/16 permanent
```

Logging options

The Status Report shows a list of the log options you configure with the Policy Manager. You can set the Firebox to record allowed and denied packets for services, intrusion detection, and many other features.

Sample

```
Logging options
Outgoing traceroute
Incoming traceroute logged(warning) notifies(traceroute) hostile
Outgoing ping
Incoming ping
```

Authentication host information

The Status Report shows which method of authentication is enabled and the IP address of the authentication server.

Sample

```
Authentication
Using local authentication for Remote User VPN.
Using radius authentication from 103.123.94.22:1645.
```

Memory

You can use the Status Report to learn how the Firebox uses its memory. The values are shown in bytes of memory.

Sample

```
Memory:
           total:   used:   free:    shared:  buffers: cached:
Mem:      65032192 25477120 39555072 9383936  9703424  362905
```

Load average

The *load average* is the average of the number of operations the Firebox does in an specified time interval. The intervals in the Status Reports are: 1, 5, and 15 minutes. The fourth and fifth numbers are shown as a pair: x/y. The fourth number is the number of current processes in the "run" state and the fifth number is the number of total processes. The last number is the Process Identification Number (PID) for the subsequent process for the Firebox to do.

Sample

```
Load Average:
0.04 0.06 0.09 2/21 6282
```

CPU Usage

The CPU Usage is the percent usage of the Firebox CPU in the last minute, 5 minutes and 15 minutes.

Sample

```
CPU Usage:
3% 5% 5%
```

Processes

The Status Report shows the Process Identification Number (PID), name and status of current Firebox operations. The report uses a status indicator in the "S" column:

- **R** — Running
- **S** — Sleeping (a process waiting for an event to complete)
- **Z** — Zombie (a process left behind by a parent process that did not close correctly)

The other fields are as follows:

- RSS — The RAM the process uses.
- SHARE — The memory that more than one process can use at the same time.
- TIME — Total CPU time used.
- (CPU) — Percentage of CPU time used.
- PRI — Priority of process.
- (SCHED) — How the process is scheduled.

Sample

```
PID NAME    S   RSS   SHARE  TIME      (CPU) PRI (SCHED)
  1 init    S   1136  564    148:41.84 ( 0)  99  (round robin)
  2 kflushd S   0     0      0:00.02   ( 0)   0  (nice)
```

Interfaces

This section shows each Firebox interface, with information about the status and packet count and any errors or collisions on the interface. If you have the Firebox X 3-Port Upgrade, the aliases eth3, eth4, and eth5 also show.

Sample

```
 Interfaces:
 lo      Link encap:Local Loopback
         inet addr:127.0.0.1  Bcast:127.255.255.255  Mask:255.0.0.0
         UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:0
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         Collisions:0
 eth0    Link encap:Ethernet  HWaddr 00:90:7F:1E:79:84
         inet addr:192.168.49.4 Bcast:192.168.49.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:3254358 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1662288 errors:0 dropped:0 overruns:0 carrier:0
         Collisions:193
```

Routes

The Status Report also includes a table of the Firebox routes.

Sample

```
Routes
Kernel IP routing table
Destination  Gateway     Genmask         Flags MSS    Window Use Iface
207.54.9.16  *           255.255.255.240 U     1500   0       58 eth0
207.54.9.48  *           255.255.255.240 U     1500   0       19 eth1
198.148.32.0 *           255.255.255.0   U     1500   0      129 eth1:0
127.0.0.0    *           255.0.0.0       U     3584   0        9 lo
```

```
default      207.54.9.30 *               UG    1500   0       95 eth0
```

ARP table

You can see the ARP table used by the Firebox.

Sample

```
ARP Table
Address           HWtype  HWaddress           Flags Mask       Iface
207.23.8.32       ether   00:20:AF:B6:FA:29   C     *          eth1
207.23.8.52       ether   00:A0:24:2B:C3:E6   C     *          eth1
```

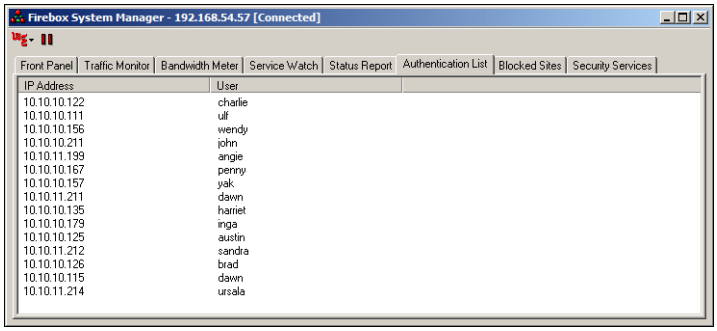
For more information on the status report page, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/log_statusall.asp

Authentication

The **Authentication List** tab of the Firebox System Manager gives the IP addresses and user names of all the persons that are authenticated to the Firebox.

You can sort users by IP address or user name by clicking the column header. You can also remove an authenticated user from the list by right-clicking on their user name and closing their authenticated session.



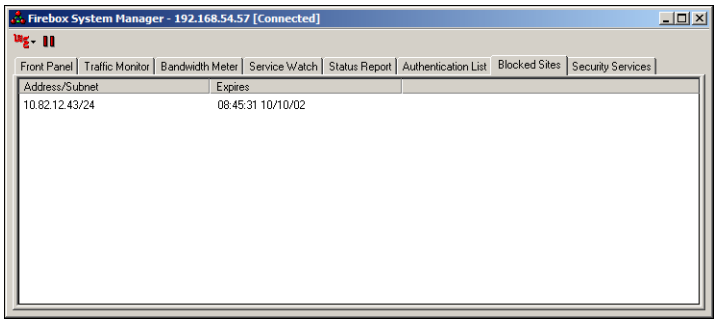
Blocked Sites

The **Blocked Sites List** tab of the Firebox System Manager shows the IP addresses of all the external IP addresses that are temporarily blocked. There are many causes for a Firebox to add an IP address to the Blocked Sites tab: a port space probe, an address space probe, an attempt to access a Blocked Port, or an event you configure.

Adjacent to each IP address is the time when it comes off the Blocked Sites list. You can use the Blocked Sites dialog box in the Policy Manager to adjust the length of time that an IP address stays on the list.

To remove an IP address from this list, right-click it and select **Remove Blocked Site**.

If you open the Firebox with the status passphrase, you must type the configuration passphrase before you can remove a site from the list.



Security Services

The **Security Services** tab lists information about the Gateway Antivirus for E-mail service. You only see this tab if you install Gateway AntiVirus for E-mail. From this tab you can:

- Update antivirus signatures
- See and clear statistics about the work Gateway AntiVirus for E-mail is doing
- Renew your Gateway AntiVirus for E-mail license

For more information about these tasks, see "Getting Gateway AntiVirus for E-mail Status and Updates" on page 172

HostWatch

HostWatch is a graphic user interface that shows the network connections between the Firebox interfaces. HostWatch also gives information about users, connections, and network address translation (NAT).

HostWatch shows all incoming and outgoing denied and allowed connections. It can show the friendly name (host name) of the inside and outside IP addresses.

The line that connects the source host and the destination host uses a color that shows the type of connection. You can change these colors. The default colors are:

- **Red** — The Firebox denies the connection.
- **Blue** — The connection uses a proxy.
- **Green** — The Firebox uses NAT for the connection.
- **Black** — A connection that is none of the first three.

Icons that show the type of service appear adjacent to the server entries for HTTP, Telnet, SMTP, and FTP.

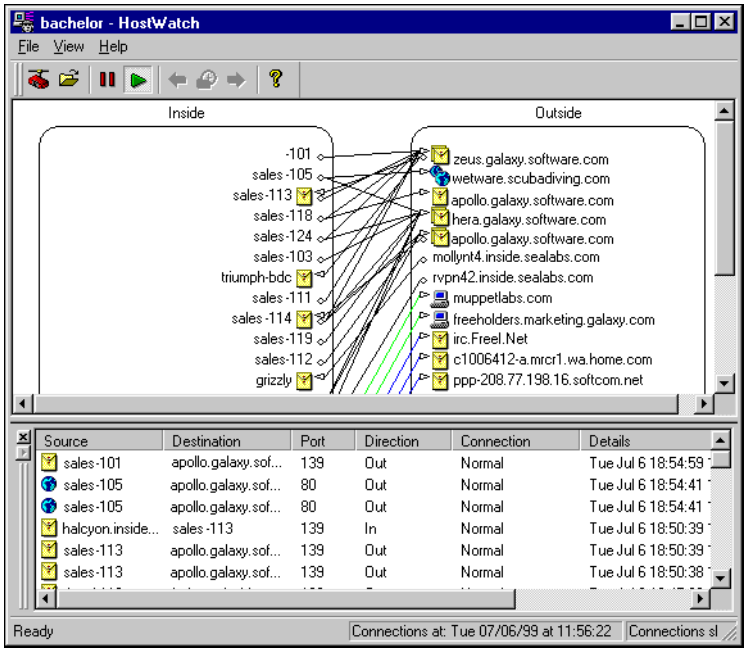
Domain name resolution (DNS) does not occur immediately when you first start HostWatch. When HostWatch does DNS, it replaces the IP addresses with the host or user names. However some IP addresses do not have DNS entries. When the computer that uses HostWatch can not identify the host or user name, the IP addresses stay in the HostWatch window.

To start **HostWatch**, click the **HostWatch** icon on the WatchGuard System Manager.

HostWatch

The top part of the HostWatch window is divided into two sides, Inside and Outside. Double-click an item on one of the sides to get a pop-up window. The window shows information about the connection, and includes the IP addresses, port number, connection type, and direction.

The lower part shows the same information in a table with the ports and the time the connection was made.



Connecting HostWatch to a Firebox

Once you launch HostWatch, you can connect to a different Firebox.

1 From HostWatch, click **File** > **Connect**.
You can also click the Connect button on the HostWatch toolbar. The Connect to Firebox dialog box appears.

2 From the **Firebox** drop-down list, select a Firebox.
You can also type the Firebox name or its IP address.

3 In the **Passphrase** text box, type the Firebox status passphrase. Click **OK**.
HostWatch connects to the Firebox and starts to show connections from the trusted and optional networks to the external network.

Controlling the HostWatch window

You can change the HostWatch window to show only the necessary items. You can use this feature to monitor only specified hosts, ports, or users.

1 From HostWatch, click **View** > **Filters**.

2 Click the tab you want to monitor: **Inside Hosts**, **Outside Hosts**, **Ports**, or **Authenticated Users**.

3 Clear the **Display All Hosts, Display All Ports, or Display All Authenticated Users** check boxes.

4 Type the IP address, port number, or user name to monitor. Click **Add**.
Do this for each item that HostWatch must monitor.

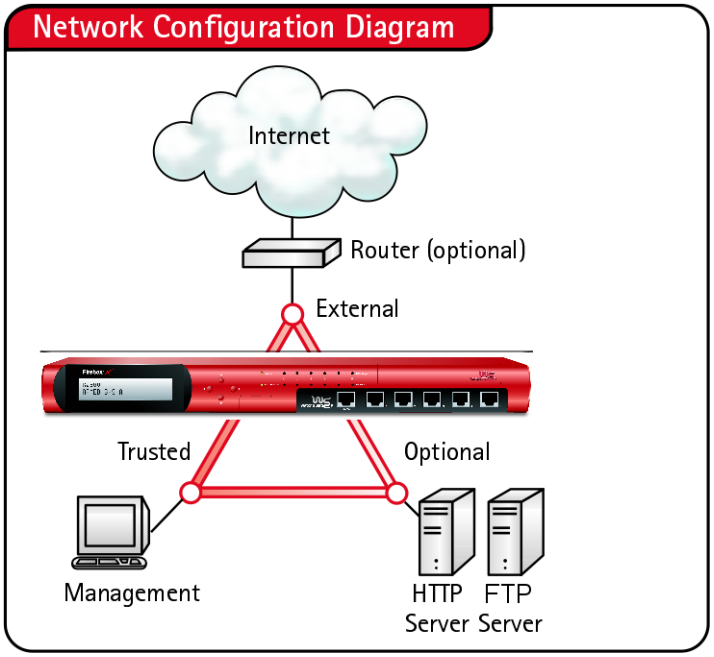
5 Click **OK**.

Changing HostWatch view properties

You can change how HostWatch shows information. For example, HostWatch can show host names as an alternative to IP addresses.

1. From HostWatch, click **View** > **Properties**.
2. Use the **Host Display** tab to change how the hosts appear in the window and the text which appears with them.
   To see the function of each control, right-click it and then select What's this?
3. Use the **Line Color** tab to change the colors of the lines between denied, dynamic NAT, proxy, and usual connections.
4. Use the **Misc.** tab to change the refresh rate of the real-time display and the maximum number of connections that show.

PART II Protecting Your Network



CHAPTER 3

Designing Your Network Architecture

This chapter gives guidance on how to add a Firebox® to your network. It includes instructions on how to:

- Use a firewall to protect and segment your network
- Select a firewall configuration mode

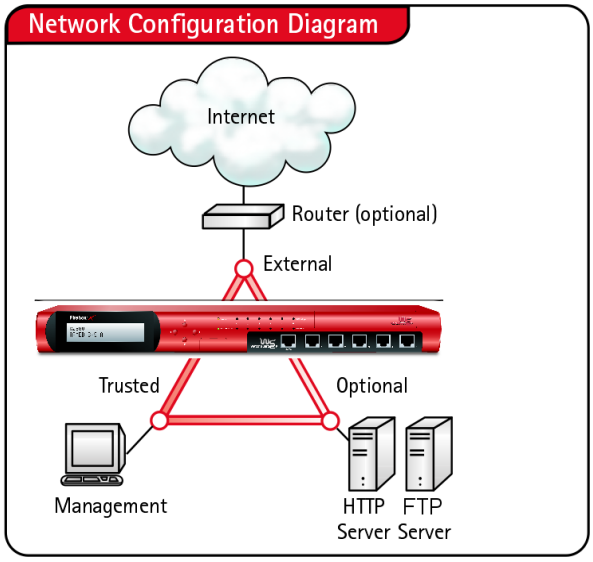
Adding a firewall to your network

A WatchGuard® Firebox® is a specially made computer which you use to protect a company network. The base model has three different interfaces. This lets you isolate your office network from the Internet. It also lets you use Web, e-mail, or FTP servers on an optional public interface. You can add more interfaces to the Firebox X with an additional license. The Firebox III has only three interfaces. The Firebox monitors each interface independently. It gives a visual indication of the operational status on the forward panel of the Firebox.

Note

There are no parts in the Firebox that a user can repair. If a user opens the case of a Firebox, the limited hardware warranty is cancelled.

The usual and best location for a Firebox is directly behind the Internet router.



The other parts of the WatchGuard System Manager are:

Management station
The computer on which you install and operate the WatchGuard System Manager software.

Management Server
The computer that controls the virtual private network tunnels that make up your distributed network. It also maintains the Certificate Authority for your network. You can configure the management station to also operate as the Management Server.

Log Server
The computer that receives and saves the log messages and sends notifications. You can configure the management station to also operate as the Log Server.

Trusted network
The network behind the firewall that must have the protection from security problems. Usually you allow no access to the trusted network.

External network
The network that is the source of your security problems, usually the Internet.

Optional network or networks
These networks have the protection of the firewall but you can allow access to them from the trusted and the external networks. You usually use the optional networks for public servers, including FTP or Web servers.

Selecting a firewall configuration mode

Before you install the WatchGuard Firebox, you must make a decision on how the firewall can be a part of your network. This decision controls the configuration of the Firebox interfaces. To install the Firebox into your network, select the configuration mode that is best for your current network.

There are two configuration modes: a routed configuration or a drop-in configuration. Many networks operate the best with a routed configuration. But we recommend the drop-in mode if:

- You have a large number of public IP addresses
- You have a static external IP address
- You can not configure the computers on your trusted and optional networks that have public IP addresses with private IP addresses.

Table 4 below shows three conditions which can help you to select a firewall configuration mode. We then give more information about each mode.

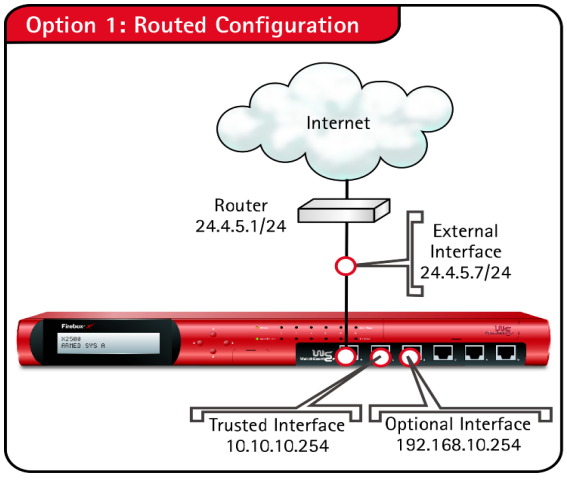
Table 4: Selecting the Configuration Mode

	Routed Configuration	Drop-in Configuration
Condition 1	All interfaces of the Firebox are on different networks. The minimum configured interfaces are external and trusted.	All interfaces of the Firebox are on the same network and have the same IP address (Proxy ARP).
Condition 2	Trusted and optional interfaces must be on different networks. The IP addresses of the interfaces must be from those networks.	The machines on the trusted or optional interfaces can have a public IP address. The two interfaces must have IP addresses on the same network.
Condition 3	Use static NAT to map public addresses to private addresses behind the trusted or optional interfaces.	The machines that have public access have public IP addresses. Thus, no static NAT is necessary.

Routed configuration

You use the routed configuration when you have a small number of public IP addresses or when your Firebox gets its external IP address using PPPoE or DHCP. For more information, see "Dynamic IP support on the external interface" on page 31. Routed configurations also make it easier to configure virtual private networking.

In a routed configuration, you install the Firebox with different logical networks and network addresses on its interfaces. The public servers behind the Firebox use private IP addresses. The Firebox uses network address translation (NAT) to route traffic from the external network to the public servers.



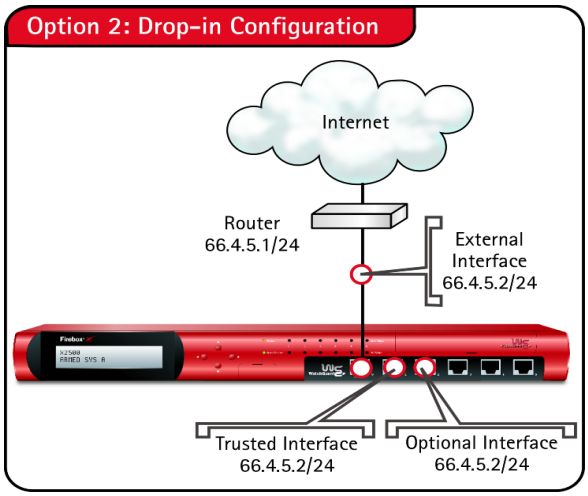
Routed Configuration Mode

The requirements for a routed configuration are:

- All interfaces of the Firebox must be on different logical networks. The minimum configuration includes the external and trusted interfaces. You can also configure one or more optional interfaces.
- All devices behind the trusted and optional interfaces must have an IP address from that network. For example, a computer on the trusted interface in Figure could have an IP address of 10.10.10.200 but not 192.168.10.200 which is on the optional interface.

Drop-in configuration

With a drop-in configuration, the Firebox uses the same network for all of its interfaces. You must configure all of the interfaces. When you install the Firebox between the router and the LAN, it is not necessary to change the configuration of the local computers. The public servers behind the Firebox continue to use public IP addresses. The Firebox does not use network address translation to route traffic from the external to your public servers.



Drop-In Configuration

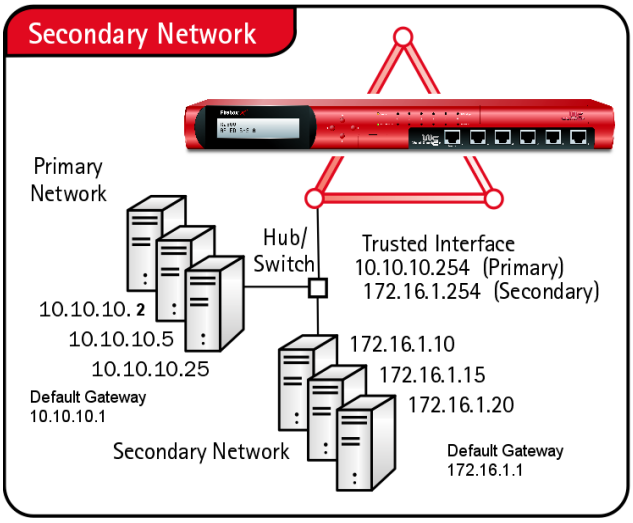
The properties of a drop-in configuration are:

- You use one logical network for all three interfaces.
- The Firebox uses proxy ARP. The trusted interface ARP address replaces the ARP address of the router. It then resolves Address Resolution Protocol (ARP) data for those devices behind the Firebox that cannot receive the transmitted data.
- During installation, it is not necessary to change the TCP/IP properties of computers on the trusted and optional interfaces. Although the router cannot receive the transmitted ARP data from the trusted host, the Firebox continues to resolve this data for the router.
- Usually, the Firebox is the default gateway as an alternative to the router.
- You must flush the ARP cache of all computers on the trusted network.
- A large part of a LAN is on the trusted interface because there is a secondary network for the LAN.

With a drop-in configuration you do not have to change the configuration of the computers on the trusted network that have a public IP address. But, a drop-in configuration is frequently not easy to manage. It can also be less easy to troubleshoot problems.

Adding secondary networks to your configuration

A secondary network is a different network that connects to a Firebox interface with a switch or hub.



When you add a secondary network, you map an IP address from the secondary network to the IP address of the Firebox interface. Thus, you make (or add) an IP alias to the Firebox interface. This IP alias is the default gateway for all the devices on the secondary network. The secondary network also tells the Firebox that there is one more network on the Firebox interface.

To add a secondary network, do one of the following:

Use the Quick Setup Wizard during installation

1 Type the IP addresses for the Firebox interfaces into the Quick Setup Wizard.

2 Select the check box if you have "an additional private network behind the Firebox".
The added private network becomes the secondary network on the trusted interface. For more information about the Quick Setup Wizard, see *WatchGuard System Manager User Guide*.

Add the secondary network after installation

Use the Policy Manager to add secondary networks to an interface. Refer to "Adding Secondary Networks" on page 60.

Dynamic IP support on the external interface

If you use dynamic IP addressing, you must select routed configuration.

If you select the Dynamic Host Configuration Protocol (DHCP), the Firebox tells a DHCP server which is controlled by your Internet Service Provider (ISP) to give it an IP address, gateway, and netmask. The DHCP server can also give WINS and DNS server information for your Firebox. If it does not give you that information, you must add it manually to your configuration. If necessary, you can change the WINS and DNS values that your ISP gives you.

Point-to-Point Protocol over Ethernet (PPPoE) is also available. As with DHCP, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. This connection automatically configures your IP address, gateway, and netmask. But, PPPoE does not give you DNS and WINS server information as DHCP does.

If you use PPPoE on the external interface, you must have the PPP user name and password to configure your network. The user name and password each have a 256-byte capacity. When you configure the Firebox to receive dynamic IP addresses, the Firebox cannot use the functions for which a static IP address is necessary: High Availability, Drop-in mode, and 1-to-1 NAT. If your ISP uses a static IP address with DHCP or PPPoE, you can enable these features because the IP address is static. For more information on enabling static DHCP or PPPoE, see "Configuring the external interface" on page 57.

Note

BOVPN with Basic DVCP is not available on Firebox III 500 unless you have the BOVPN Upgrade. It is available on the Firebox X700, Firebox X1000, and Firebox X2500 if you register the device with LiveSecurity Service.

External aliases and 1-to-1 NAT are not available when the Firebox is a PPPoE client. Manual IPSec tunnels are not available when the Firebox is a DHCP or PPPoE client.

CHAPTER 4

Basic Firebox Configuration

This chapter gives instructions for basic Firebox configuration and maintenance tasks. It includes how to:

- Open a configuration file
- Save a configuration file to a local computer or the Firebox
- Change the Firebox passphrases
- Set the Firebox time zone
- Set a Firebox special name

Opening a Configuration File

Policy Manager for the WatchGuard Firebox System is a software tool that lets you make, change, and save configuration files. A configuration file, with the extension `.cfg`, contains all configuration data, options, addresses, and other information that makes your Firebox security policy. When you use Policy Manager, you see a version of your configuration file that is easy to examine and to change.

This section tells you how to open a configuration file. You can do this only after you use the Quick Setup Wizard and save a basic configuration file to the Firebox or to your local hard drive. If you have not used the Quick Setup Wizard, refer to Chapter 5, "Use Policy Manager to Configure Your Network" for information on how to make a basic configuration.

1 Start the WatchGuard System Manager.
For more information, see the *WatchGuard System Manager User Guide*.

2 Select a Firebox with WFS appliance software in the Devices tab.

3 Select **Tools** > **Policy Manager**.

Or click the Policy Manager icon on the WatchGuard System Manager toolbar. This icon is shown at the left.

Opening a configuration from the Firebox

Policy Manager saves the configuration properties and settings in a text file with the extension .cfg. This is called the configuration file. You use Policy Manager to edit the configuration file and to save it to the Firebox.

When you select a Firebox and click the Policy Manager icon on the WatchGuard System Manager toolbar, it automatically identifies the appliance software on the Firebox and opens the correct management tool. It also loads the configuration file for that Firebox.

When you are in Policy Manager, you can also open the configuration file of another Firebox or a file you saved to your management station hard drive.

1 From Policy Manager, click **File** > **Open** > **Firebox**.
The Open Firebox dialog box appears.

2 From the **Firebox** drop-down list, select a Firebox.
You can also type the IP address or host name.

3 In the **Passphrase** text box, type the Firebox status (read-only) passphrase. Click **OK**.
Use the status passphrase to monitor traffic and Firebox condition. You must use the configuration passphrase to save a new configuration to the Firebox.

4 If necessary, type a value in the **Timeout** field. This value sets the time (in seconds) that the management station listens for data from the Firebox before it sends a message that shows that it cannot get data from the device.

Opening a configuration from a local hard disk

1 Click **File** > **Open** > **Configuration File**.

2 Find and select the configuration file you want to open, and then click **Open**.

Saving a Configuration File

After you make a change to a configuration file, you can save it directly to the Firebox®. You can also save it to a local hard disk. When you save a new configuration file directly to the Firebox, Policy Manager can tell you that you must restart the Firebox. If Policy Manager tells you to restart the Firebox, the new security policy starts only after you restart the Firebox.

If Policy Manager does not tell you to restart the Firebox, the new security policy starts when the Save operation is complete.

If the software version number on the management station is different from the version number on the Firebox, you must save a new flash image. For information on how to update the Firebox to a new version of the software, see the FAQ:

www.watchguard.com/support/advancedfaqs/flashdisk_update.asp

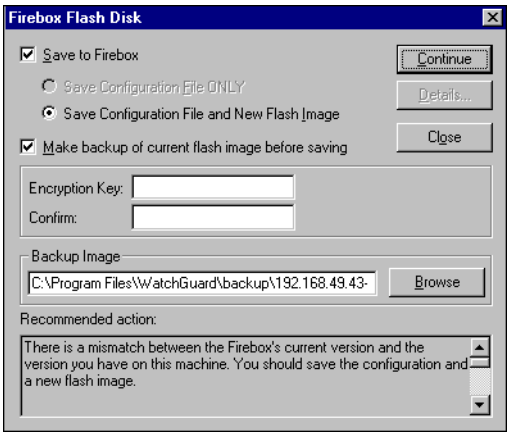
Saving a configuration to the Firebox

1 From Policy Manager, click **File** > **Save** > **To Firebox**.
You can also press CTRL-T.

2 From the **Firebox** drop-down list, select a Firebox.
When you type an IP address, type all the numbers and the dots. Do not use the TAB key or arrow key.

3 In the **Passphrase** text box, type the Firebox configuration (read/write) passphrase, and then click **OK**.
The configuration file saves to the local hard disk and then to the primary area of the Firebox flash disk. This causes the software to tell you to save the configuration file to the Firebox, which replaces the configuration that is on the Firebox.

4 If you typed the IP address of a different Firebox, you must confirm your selection. Click **Yes**.
The Firebox Flash Disk dialog box appears. See the figure below.


Firebox Flash Disk
Save to Firebox
Save Configuration File ONLY
Save Configuration File and New Flash Image
Make backup of current flash image before saving
Continue
Details...
Close
Encryption Key:
Confirm:
Backup Image
C:\Program Files\WatchGuard\backup\192.168.49.43-
Browse
Recommended action:
There is a mismatch between the Firebox's current version and the version you have on this machine. You should save the configuration and a new flash image.

5 Select the **Save To Firebox** check box. To make a backup flash image before you replace it with the new configuration file, click **Make Backup of Current Flash Image**.

Note

It is not necessary to make a backup of the current flash image each time you change the configuration file. When you back up the current flash image, you must enter an encryption key. It is important you remember this key. You must use this key to restore the Firebox if you save a defective configuration file to the device.

6 If you do not make a backup flash image, click **Continue**. If you do make a backup flash image, type the encryption key for the Firebox in the **Encryption Key** text box. In the **Confirm** text box, type the key again to confirm.

7 If you make a backup flash image, type the path to save the backup image in the **Backup Image** text box. Click **Continue**.
You can click Browse to select the location of the backup image.

8 In the **Passphrase** text box, type the Firebox status (read-only) passphrase and the Firebox configuration (read/write) passphrase. Click **OK**.
The new flash image saves to the Firebox.

Note

When you make regular changes to a configuration file, a new flash image is not necessary. If you click Save Configuration File Only, that is usually sufficient.

Saving a configuration to the management station

From Policy Manager:

1 Click **File** > **Save** > **As File**.
You can also use CTRL-S. The Save dialog box appears.

2 Type the name of the file.
The default procedure is to save the file to the WatchGuard directory.

3 Click **Save**.
The configuration file saves to the local hard drive.

Changing the Firebox passphrases

WatchGuard recommends that you change the Firebox® passphrases at regular intervals. To do this, you must have the configuration passphrase. From Policy Manager:

1 Open the configuration file from the Firebox.
For more information, refer to "Opening a configuration from the Firebox" on page 34.

2 Click **File** > **Save** > **To Firebox**.

3 From the **Firebox** drop-down list, select a Firebox or type the IP address of the Firebox. Type the Firebox configuration (read/write) passphrase. Click **OK**.
The Firebox Flash Disk dialog box appears.

4 Select the **Save To Firebox** check box. Click **Save Configuration File and New Flash Image**. Clear the **Make Backup of Current Flash Image** check box. Click **Continue**.

5 Type and confirm the new status (read-only) and configuration (read/write) passphrases. The status passphrase must be different from the configuration passphrase. Click **OK**.
The new flash image and the new passphrases save to the Firebox. The Firebox automatically starts again.

Making your passphrases safer

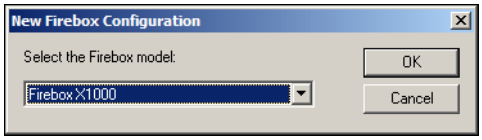
To create a secure passphrase, we recommend that you:

- Do not use words from standard dictionaries even if you use them in a different sequence or in a different language. Make a new acronym that only you know.
- Do not use a name. It is easy for a hacker to find a business name, familiar name, or the name of a famous person.
- Use a selection of uppercase and lowercase characters, numbers, and special characters (for example, Im4e@tiN9).

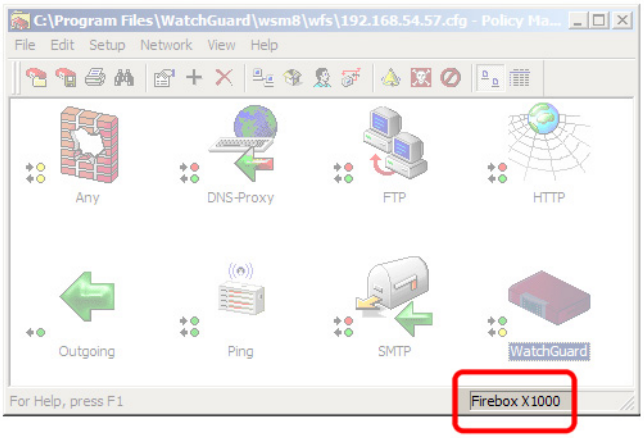
Setting the Firebox Model

You select the Firebox® model only when you start a new configuration file or when you open a configuration file. You can change the Firebox model if you save a configuration file from one Firebox to a different model Firebox.

1 From Policy Manager, click **Setup** > **Firebox Model**.
The New Firebox Configuration dialog box appears.



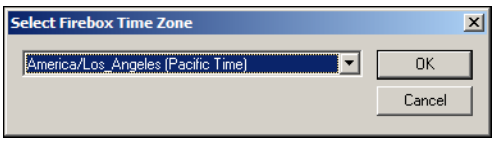
2 Select the Firebox model to which you will connect.
The Firebox model appears at the lower-right corner of the Policy Manager window.



Setting the Time Zone

The Firebox® time zone controls the date and time that appear in the log file and on tools that include Log Viewer, Historical Reports, and WebBlocker. The default time zone is Greenwich Mean Time (Coordinated Universal Time).

1 From Policy Manager, click **Setup** > **Time Zone**.



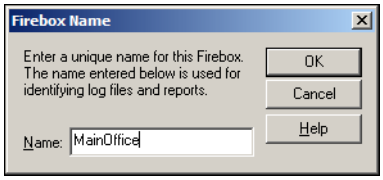
2 Select a time zone from the drop-down list. Click **OK**.

Setting a Firebox Friendly Name

You can give the Firebox a special name to use in your log files and reports. Many customers use the external IP address of the Firebox. You can also use a Fully Qualified Domain Name if you register such a name with the DNS system. If you do not set this name, some features cannot operate correctly.

1 From Policy Manager, click **Setup** > **Name**.
The Firebox Name dialog box appears.

2 In the **Name** text box, type the special name you want for the Firebox. Click **OK**.
You can use all characters but spaces and slashes (/ or \).



CHAPTER 5

Using Services to Create a Security Policy

A *service* is a group of rules for how a firewall routes your network traffic. The parameters of a service include:

- Direction of traffic (incoming or outgoing)
- Firebox action (enabled and allowed, enabled and denied, disabled)
- Source and destination
- One or more ports
- One or more protocols
- Log and notification properties

Packet Filters and Proxies

In Policy Manager for WFS, there are two categories of services: packet filters and proxies.

A *packet filter* examines each packet header. A packet filter is the most basic feature of a firewall. It controls the network traffic into and out of your Firebox®. It can also record a log message or send a message to the source.

A *proxy* examines each packet header and the content of each packet. If the content does not match the rule criteria you set, the Firebox denies the packet. A proxy operates at the application layer, while a packet filter operates at the network layer and transport layer. When you enable a proxy, the Firebox:

- Removes all the network data
- Examines the contents for RFC compliance and content type matches.
- Restores the network data
- Sends the packet to its initial destination

A proxy uses more resources and bandwidth than a packet filter. But, a proxy can catch dangerous content types that a packet filter cannot.

Services and the Policy Manager

In this *Configuration Guide*, we refer to packet filters and proxies together as services. Unless we tell you differently, the procedures below refer to proxies and packet filters.

The Policy Manager shows each packet filter and proxy as an icon. You configure the rules for outgoing traffic and incoming traffic. The traffic can be allowed or denied, and you can configure the source and destination. You can also set the rules for your log messages and notification messages, and for computer ports, protocols, and other packet properties.

Selecting Services for your Security Policy

WatchGuard® System Manager denies all packets that are not specially approved. You see this policy in network security documentation as:

If you do not allow a given traffic type, it is denied.

This security policy helps to protect your network from:

- Attacks with a new service or different IP service
- Unknown services
- Configuration errors

When you configure the Firebox® with the Quick Setup Wizard, you set only the basic packet filters and interface IP addresses. To allow more traffic through the Firebox, you must:

- Configure the services and protocols on the Firebox to let necessary traffic through
- Set the approved hosts and properties for each service or protocol
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

Incoming and outgoing services

A connection from a less trusted segment of the network to a more trusted segment is *incoming*. You must configure an incoming connection on the Incoming tab for the service. A connection from a more trusted segment to a less trusted segment is *outgoing*. You must configure an outgoing connection on the Outgoing tab for the service.

For example, to let a telnet connection through the Firebox from the eth5 optional network to the eth2 optional network is incoming. This is because the data flow is from a less trusted network to a more trusted network.

Or, you can allow an HTTP connection from a VPN source through the Firebox to the external interface. Here, you use the Outgoing tab for the HTTP service, because VPN sources are more trusted than external sources.

For more information on incoming traffic and outgoing traffic and how they apply to the different Firebox interfaces, refer to "About Incoming and Outgoing Traffic" on page 4.

Incoming service guidelines

When you enable an incoming service, you create a small hole into your network. The guidelines below can help you to make an estimate of the security risks as you add each incoming service. Each safety precaution you add gives you a safer network. To follow three or four precautions is much safer than to follow one or none.

- Your total security is only as high as the service you allow with the lowest security properties.
- Do not trust traffic sources that you do not know.

- If you know more about a software application and the network traffic it uses, you can configure a better security policy.
- Services with no built-in authentication and that are not created for use on the Internet are a risk.
- Services that send your password in clear text such as FTP, Telnet, POP are a high risk.
- Services with built-in strong authentication such as ssh are more safe. If the service does not have built-in authentication, you can decrease the risk if you use user authentication with that service.
- Services such as DNS, SMTP, anonymous FTP, and HTTP are safe only if you use them correctly as designed.
- You can decrease your risk if you let an incoming service connect to one trusted computer. The more internal computers you allow the service to connect to, the more you are at risk.
- You can decrease your risk if you let an incoming service come from only IP addresses you select. The more external IP addresses you allow, the more you are at risk.
- You can decrease your risk if you use authentication. If you do not have an authentication server, you can use Firebox authentication, included with WatchGuard System Manager.
- To open access to the optional network is safer than to open access to the trusted network.

Outgoing service guidelines

Usually, an incoming service adds the highest risk, but there can also be a risk with an outgoing service. For example, when you configure the outgoing FTP service, you can make it a read-only service or set a limit on the destination hosts. This prevents your users from downloading a virus or software application from an FTP site. One more example: some services (FTP, telnet, POP) send your passwords using a method in which they are easily read. If the passwords are the same as the ones you use internally, a hacker can get your password and use it to get access to your network.

Many of the guidelines shown above for an incoming service are also valid for an outgoing service. The basic rule is that "less is more." The less services you add to your Firebox configuration, the more secure your network.

Adding and Configuring Services

You can add and configure services with Policy Manager for WFS. You can see the icons that identify services you have configured in the Policy Manager.

For each service you can:

- Set allowed traffic sources and destinations (incoming and outgoing)
- Make filter rules and policies
- Enable or disable the service

The Policy Manager includes many pre-configured packet filters. For example, to apply a packet filter to all Telnet traffic, you can easily add a Telnet packet filter. You can also make a custom packet filter for which you set the ports, protocols and other parameters.

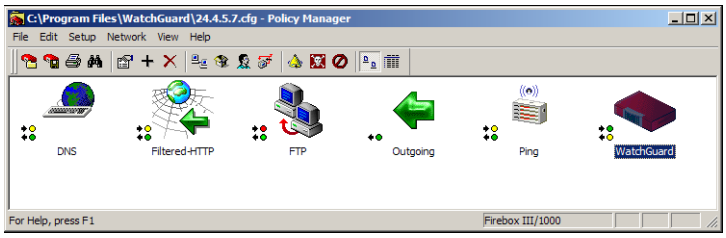
For more information on pre-configured services, see Appendix A of this guide. You can also refer to the Services FAQ:

https://www.watchguard.com/support/advancedfaqs/svc_main.asp

Changing the Policy Manager View

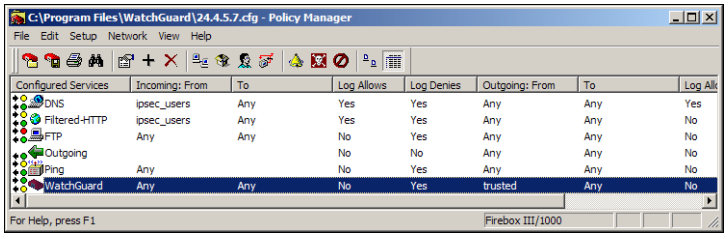
The Policy Manager has two views: **Large Icons** view and **Details view**. The Large Icons view shows each service as an icon. Two small dots are the status indicators. They show if the service allows or denies incoming traffic and outgoing traffic.

To change to the Large Icons view, click the **Large Icons** button on the toolbar.



Large Icons View of Policy

To change to the Details view, click the **Details** button on the toolbar. In the Details view, each service is a row. You can see configuration information such as source and destination, and log and notification properties.


C:\Program Files\WatchGuard\24.4.5.7.cfg - Policy Manager
File Edit Setup Network View Help
Configured Services
Incoming: From
To
Log Allows
Log Denies
Outgoing: From
To
DNS ipsec_users Any Yes Yes Any Any Yes
Filtered-HTTP ipsec_users Any Yes Yes Any Any No
FTP Any Any No Yes Any Any No
Outgoing No No Any Any No
Ping Any No Yes Any Any No
WatchGuard Any Any No Yes trusted Any No
For Help, press F1
Firebox III/1000

Details View of Services Arena

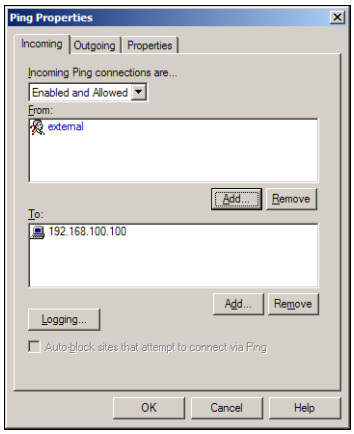
Service Parameters to Configure

You can configure most parameters of a packet filter or proxy service. In the subsequent chapter, "Configuring Proxied Services," on page 69, you can learn more about the proxy parameters. This section is about the properties that are the same for all services.

When you open a service icon, you see three tabs: Incoming, Outgoing, and Properties.

Incoming

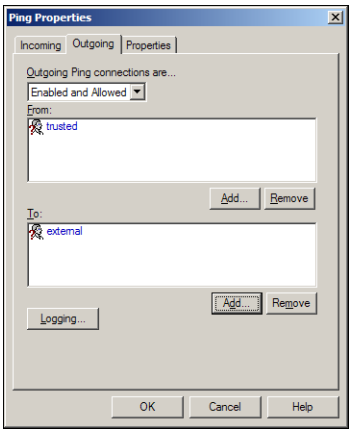
Use the Incoming tab to enable traffic from the less trusted network to the more trusted network. For example, you can configure incoming traffic from the external network to the trusted network.



On the **From** list, you add the computers and networks that can send incoming traffic using this service. On the **To** list, you add the computers and networks to which the Firebox can route traffic with this service. For example, you could configure an incoming ping packet filter to allow ping traffic from all computers on the external network to one Web server on your optional network.

Outgoing

Use the Outgoing tab to enable traffic from the more trusted network to the less trusted network. For example, you can configure outgoing traffic from the trusted network to the optional network.



On the **From** list, you add the computers and networks that can send outgoing traffic with this service. On the **To** list, you add the computers and networks to which the Firebox can route traffic using this service. For example, you could configure an outgoing ping packet filter to allow computers on the trusted network to ping computers on the external network.

Logging

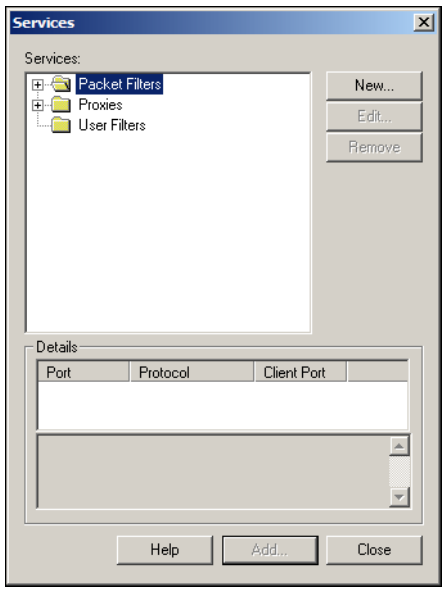
For each service, you select the events that cause the Firebox to send a log message. You can also set the Firebox to send an e-mail message or other notification.

Adding a service

You use the Policy Manager to add a packet filter or proxy to your configuration. To add a service:

1 From Policy Manager, select **Edit** > **Add Service**.

Or
Click the Add service icon on the Policy Manager toolbar. The icon is shown at left.
The Services dialog box appears.



2 Click the plus (+) sign on the left side of the folder to expand the **Packet Filters** or **Proxies** folders.
A list of the packet filters or proxies appears.

3 Click the name of the service to add.
When you select a service, the service icon appears in the area below the New, Edit, and Remove buttons. Also, the Details box shows basic information about the service.

4 Click **Add**.
The Add Service dialog box appears.

5 You can change the name and information that appear when you configure the service. This information appears in the Policy Manager Details view. Click the **Name** or **Comment** text box and type the values.

6 Click **OK**.
The Properties dialog box of the service appears. For more information on how to configure the service properties, refer to "Adding service properties" on page 48.

7 Click **OK** to close the **Properties** dialog box.
You can add more than one service while the Services dialog box is open.

8 Click **Close**.
The new service appears in the Policy Manager.

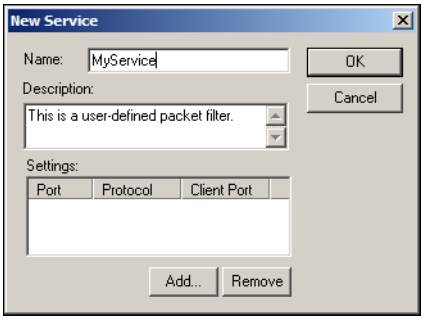
Making a new service

The Policy Manager includes many pre-configured packet filter services, but you can also make a new service. You can also change a pre-configured service. It can be necessary to do this if you add a new software application behind your firewall. Remember, each new service can increase your security risk.

1 From Policy Manager, select **Edit** > **Add Service**.

Or
Click the Add service icon on the Policy Manager toolbar. The icon is shown at left. The Services dialog box appears.

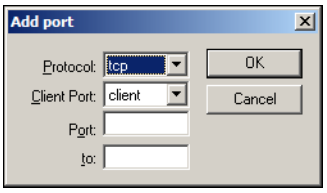
2 Click **New**.
The New Service dialog box appears.



3 In the **Name** text box, type the name of the service.
This name must not be the same as names in the list in the Services dialog box. The name appears in the Policy Manager and it helps you to find the service when you must change or remove it.

4 In the **Description** text box, type a description of the service.
This appears in the Details section when you click the service name in the list of User Filters.

5 To set up the port for this service, click **Add**.
The Add Port dialog box appears.



6 From the **Protocol** drop-down list, select the protocol for this new service. For more information about network protocols, see the *Reference Guide* or online help system. You can select:
- **TCP** The firewall examines TCP packets.
- **UDP** The firewall examines UDP packets.
- **HTTP** The firewall examines TCP packets with the HTTP Proxy.
- **IP** Set the firewall to examine packets for a different protocol. You select **IP** to create a protocol number service. Examples include GRE (IP 47) and ESP (IP 50). The **Next-level** field appears in the **Add Port** dialog box. Type the number of the protocol.

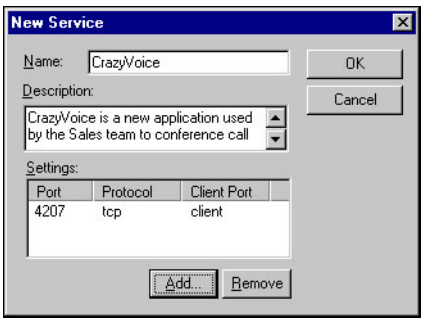
7 From the **Client Port** drop-down list, select the client port for this new service. Note that you can select one port or a range of ports. For the Client Port, you can select:
- **Ignore** The source port range is from 0–65565. Use this if you are not sure which port to use.
- **Secure** The source port range is from 0–1024 (not usually used).
- **Port** The source port must be the same as the destination port. This shows in the **Port** number field of the **Properties** dialog box of the destination service (not usually used).
- **Client** The source port range is from 1025–65565.

8 In the **Port** text box, type the port number.

9 To set a range of port numbers, type the lowest number of the range in the **Port** text box. In the **To** text box, type the highest number of the range.

10 Click **OK**.

The Policy Manager adds the values to the New Service dialog box. Make sure that the name, information, and configuration of this service are correct. You can click Add to configure more ports for this service. Complete the Add Port procedure again until you configure all ports for the service.



11 Click **OK**.

The Services dialog box appears with the new service in the User Filters folder. You can at this time add one or more services using the new service dialog box.

12 In the **Services** dialog box, expand the **User Filters** folder. Click the name of the service. Click **Add**. Click **OK** to close the **Add Service** dialog box. Click **OK** to close the **Properties** dialog box. Click **Close** and the **Services** dialog box closes.

The icon of the new service appears in the Policy Manager.

Adding more than one service of the same type

To match the requirements of your security policy, you can add the same service many times. For example, you can set a limit on the use of the Web for most users, while you give your management complete use of the Web. To do this, you make two different HTTP services with different properties for the outgoing rule:

1 Add the first service. Refer to steps 1 – 4 in "Adding a service" on page 44.

2 Change the name of the service to give its function in your security policy and add the related information.

In the first example of the different HTTP services, you can give the first HTTP service the name "restricted_web_access."

3 Click **OK.** The **Properties** dialog box of the service appears. Set the outgoing properties. Refer to "Adding service properties" on page 48.

In the example, you can add an alias "staff," which has a range of IP addresses or a group of authenticated users. For more information on aliases, refer to "Using Aliases" on page 93.

4 Add the second HTTP service.

In the example, you can give this second HTTP service the name "full_web_access."

5 Click **OK.** The **Properties** dialog box of the service appears. Set the outgoing properties. Refer to "Adding service properties" on page 48.

In the example, you can add an alias "executives".

Note

Do not create services that do the opposite. For example, do not create one HTTP service that lets incoming traffic through while the other denies incoming traffic. You can use the Disabled option to prevent this.

Deleting a service

As your security policy changes, it could be necessary to remove one or more services. To remove a service, you must first remove it from the Policy Manager. Then you must save the new policy to the Firebox.

From Policy Manager:

1 Click the icon of the service want to remove.

2 From Policy Manager, select **Edit** > **Delete**.

Or
Click the Delete Service icon on the Policy Manager toolbar. The icon is shown at left. The Services dialog box appears.

3 To confirm, click **Yes**.

4 Save the configuration to the Firebox and start the Firebox again. Click **File** > **Save** > **To Firebox**. Type the configuration passphrase. Select the **Save to Firebox** check box. Click **Save**.

Configuring Service Properties

You can use the service **Properties** dialog box to configure incoming and outgoing access rules for a given service.

The **Incoming** tab shows:

- The sources on the external network (or a less trusted network) that use this service to start a connection with the users, hosts, and networks behind the Firebox®.
- The destinations behind the Firebox for the incoming traffic for this service.

The **Outgoing** tab shows:

- The sources behind the Firebox that use this service to start a connection with an external (or less trusted) destination.
- The destinations on the external network for the outgoing traffic for this service.

A service can be:

Disabled
The Firebox does not examine the traffic using this service. The Disabled option lets you make a service that examines traffic in only one direction.

Enabled and Denied
The Firebox denies all traffic using this service. You can configure it to record a log message when a computer tries to use this service. It can also automatically add a computer or network that tries to start a connection with this service to the Temporary Blocked Sites list.

Enabled and Allowed
The Firebox allows traffic using this service if it obeys the rules you set for source and destination.

Opening the Service Properties dialog box

When you add a service, the **Properties** dialog box of the service automatically appears. To show the **Properties** dialog box of a service, you can double-click the service icon in the Policy Manager. Also, you can click the services icon and click the Edit Service button.

Adding service properties

The procedure to add incoming and outgoing service properties is the same.

1 Double-click the service icon to open the Service Properties dialog box.

2 Click the tab with the properties you want to change.

3 Click **Add** for the **From** or the **To** member list.

4 Set the members for the service.

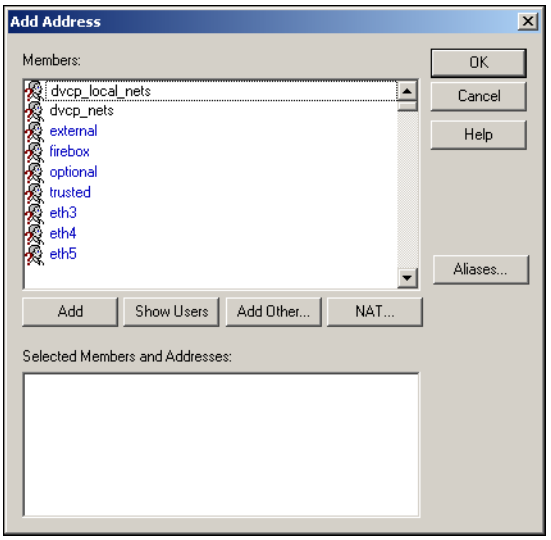
Tab	Member List	Users
Incoming	From	The computers, networks, and users on the less trusted network that can send incoming traffic
Incoming	To	The destinations on the more trusted network which can receive incoming traffic
Outgoing	From	The computers, networks, and users on the more trusted network than can send outgoing traffic
Outgoing	To	The destinations on the external network which can receive outgoing traffic

Adding addresses or users to service properties

The Incoming properties and Outgoing properties include From and To address lists. Use the **Add Address** dialog box to add a network, IP address, or specified user to a service. From the **Properties** dialog box:

1 From the **Incoming service Connections Are** drop-down list, select **Enabled and Allowed**.

2 Click the **Incoming** tab or **Outgoing** tab. Click **Add** (below the **From** or **To** list).
The Add Address dialog box appears.



3 Click **Add Other**.

4 From the **Choose Type** drop-down list, select the address type, range, host name, or user to add.

5 In the **Value** text box, type the correct address, range, or name. Click **OK**.
The member or address appears in the Selected Members and Addresses list.

6 Click **OK**.
The new selection appears in the Incoming or Outgoing tab below the From or To box.

Working with wg_icons

When you enable some features of the WatchGuard System Manager, the Policy Manager automatically adds a service. These WatchGuard service names start with "wg_" and include PPTP and authentication. WatchGuard recommends that you keep the default parameters of these automatically created icons.

wg_ icons appear in the Policy Manager if you click **View** > **Hidden Services**. A check mark appears adjacent to the menu selection. To hide wg_ icons, click **View** > **Hidden Services** again. The check mark clears.These are wg_ services:

wg_authentication
Appears when you enable user authentication.

wg_dhcp_server
Appears when you enable the DHCP server.

wg_pptp
Appears when you enable PPTP.

wg_mgmt_server
Appears when you configure the WatchGuard Management Server, to allow connections between the Management Server and its clients.

wg_webblocker
Appears when you use WebBlocker to allow database updates.

Customizing logging and notification

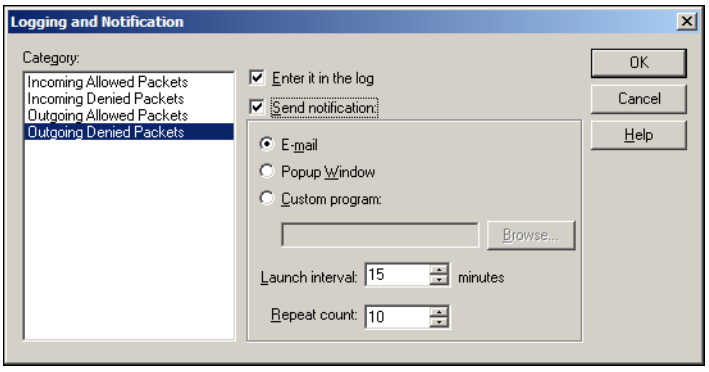
In WatchGuard System Manager you can set custom log properties and notification properties for each packet filter and proxy. You can also configure the log messages for other features. Use the **Logging and Notification** dialog box to configure the Firebox to record the usual network traffic events and to send a notification only for a very important event.

The Policy Manager uses almost the same dialog box for all services, options, and features. Thus, if you know the parameters for one service type, you can easily configure the remaining services.

1 Double-click the service icon to open the Service Properties dialog box.

1 Click the **Incoming** tab. Click **Logging**.
The Logging and Notification dialog box appears.

2 Set the parameters and notification to match the requirements of your security policy.



Category

A list of the categories of traffic for which the Firebox can record a log message. This list is different for each service or selection. Click the category name to show and select the parameters.

Enter it in the log

When you enable this check box, the Firebox sends a log message when it sees a traffic type that matches the one you selected in the Category list. The default configuration of all services is for the Firebox to send a log message when it denies a packet.

Send notification

When you enable this check box, the Firebox sends a notification when it sees a traffic type that matches the one you selected in the Category list. You set the notification parameters with the WatchGuard Log Server. For more information, see the logging chapters in the *WatchGuard System Manager User Guide*.

You can configure the Firebox to do one of these actions:

- **E-mail** The Firebox makes the management station send an e-mail message when the event occurs. Set the e-mail address in the **Notification** tab of the WSEP user interface.
- **Pop-up Window** The Firebox makes a dialog box appear on the management station when the event occurs.
- **Custom Program** The Firebox starts a software application or script when the event occurs. You must type the full path to the file, or use **Browse** to find and select the file.

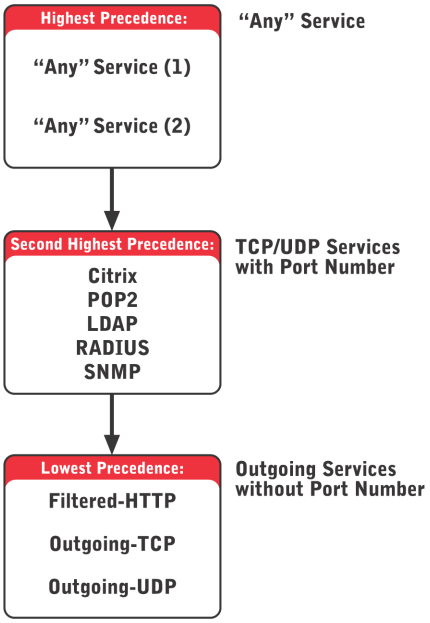
You can control how frequently a notification will be sent, together with the Repeat Interval.

Service Precedence

The service precedence is the sequence in which the Firebox sorts more than one service. The Firebox gives precedence to the most tightly configured service and moves down to the most general service. For example, a service with one source IP address to one destination IP address has a higher precedence than the same service with a configuration from any computer to any computer.

The Firebox also gives precedence by group. There are three different precedence groups.

- The **Any** service has the highest precedence. For more information about the Any service, see *Appendix A of this guide*.
- IP and ICMP services and all TCP/UDP services that have a specified port number have the second highest precedence. This is the largest precedence group.
- The **Outgoing** services that do not give a port number have the lowest precedence. This group includes Outgoing TCP, Outgoing UDP, and Proxy.



A service can contain rules from more than one precedence group. For example, the Filtered-HTTP packet filter and the Proxied-HTTP proxy contain a TCP rule for port 80 and a rule with no specified port for all other TCP connections. When there is more than one rule, the Firebox uses the one with the highest precedence first. The Blocked Sites list has precedence over the Any service, and all other services.

Because the Firebox sorts your services from the most tightly configured service to the most general service, the table below gives a general guidelines for precedence when you have two or more of the same service:

From	To	Rank
IP	IP	0
List	IP	1
IP	List	2
List	List	3
Any	IP	4
IP	Any	5
Any	List	6
List	Any	7
Any	Any	8

IP refers to one host IP address

List refers to more host IP addresses, a network address, or an alias

Any refers to the special "Any" target (not "Any" services)

The Firebox always examines the highest precedence service first. If it does not agree, it examines the subsequent service, and continues to examine services until one matches. If the Firebox finds no service match, it denies the packet.

For example, there are two Telnet icons:

- telnet_1: that lets traffic go from A to B.
- telnet_2: that lets traffic go from C to D.

When the Firebox receives a Telnet packet from C with a destination of E, first it examines the telnet_1 service rule. Then it examines the telnet_2 service rule. Because this packet does not match telnet_1 or telnet_2, the Firebox denies the packet.

When only one icon shows a service, WatchGuard System Manager only examines that service. If the packet agrees with the service, and the source and destination, the service rule applies. If the packet agrees with the service, but does not agree on the source or destination, the packet is denied.

For example, if one Telnet icon lets traffic go from A to B, a Telnet try from A to C is blocked. System Manager does not examine the lower-precedence services for agreement, including outgoing services.

For more information on the outgoing services, refer to the FAQs:

www.watchguard.com/support/advancedfaqs/svc_outgoing.asp
www.watchguard.com/support/AdvancedFaqs/svc_precedence.asp

CHAPTER 6

Configuring the Network Interfaces

Usually, when you install the Firebox® in your network you use the Quick Setup Wizard to make a basic configuration file. For more information, see *WatchGuard System Manager User Guide*. But, you also can use the Policy Manager to make a basic configuration file or to change one you made with the Quick Setup Wizard.

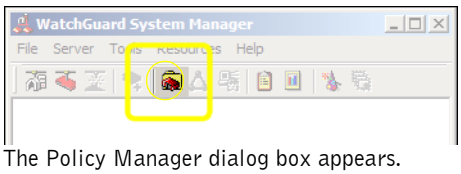
If you are new to network security, we recommend that you do these steps in the sequence in this chapter to make sure you configure all the components of your network. In this chapter, we learn how to use the Policy Manager for WFS to:

- Make a new configuration file
- Configure the Firebox interfaces
- Add a secondary network
- Add DNS and WINS server information
- Configure the Firebox as a DHCP server
- Add basic services to Policy Manager
- Configure routes

Making a New Configuration File

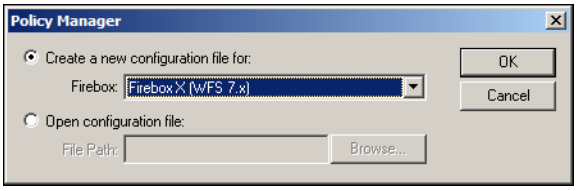
A new configuration file contains the default parameters for the specified Firebox model. To make a new configuration file:

1 From WatchGuard System Manager, click the Policy Manager icon on the toolbar.



The Policy Manager dialog box appears.

2 From the **Policy Manager** dialog box, select the model of your Firebox. If you have a Firebox X, select Firebox X (WFS 7.x).



3 Click **OK**.
The Policy Manager opens with a default configuration file for the model selected.

4 We recommend that you save the configuration file frequently. From Policy Manager, click **File** > **Save** > **As File**. Save the file as a unique name to your local hard drive.

Setting the IP Addresses of Firebox Interfaces

The selected configuration mode controls the procedure that you use to set the IP addresses for the Firebox® interfaces.

Note

Before you set the IP addresses for the Firebox interfaces, you must make a decision on your configuration mode. If you use an incorrect IP address, it can cause problems. For more information, refer to "Select a Firewall Configuration Mode" on page 26.

Setting addresses in drop-in mode

You use the drop-in mode when you want to put computers that use the same network on different Firebox interfaces. Usually, you use this mode when:

- You have many servers with public IP addresses on them
- You want to "drop" the Firebox into your network.
- You do not want to change the network configuration on the public servers.

With a drop-in configuration, the Firebox uses the same IP address and subnet mask for all of its interfaces. You indicate the subnet mask using slash notation.

The subnet mask shows the range of IP addresses in the drop-in network. For example, if you give the Firebox the IP address 1.1.1.5/24, this means that all Firebox interfaces have IP address 1.1.1.5. The drop-in network includes IP addresses from 1.1.1.1 to 1.1.1.254. The /24 indicates subnet mask 255.255.255.0.

When you use the drop-in configuration, a computer with an IP address in the drop-in network can go on any Firebox interface. When you install the Firebox between the router and the LAN, it is not necessary to change the configuration of a local computer if it has an IP address in the drop-in network. The public servers behind the Firebox can continue to use public IP addresses in the drop-in network range.

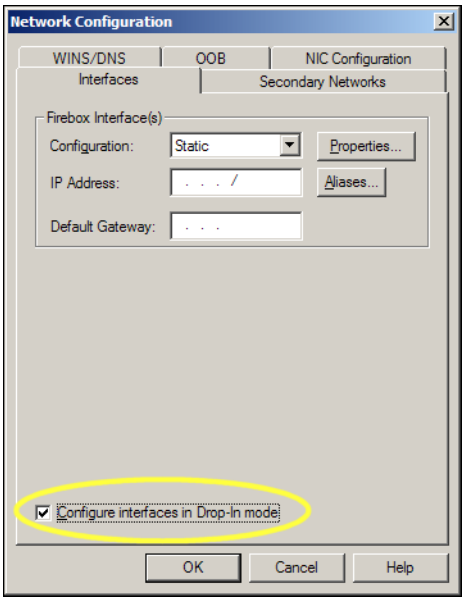
You can also put computers on the same LAN that use IP addresses from a different network. See "Adding Secondary Networks" on page 60.

To use the Policy Manager to set the Firebox in drop-in configuration mode:

1 Click **Network** > **Configuration**.
The Network Configuration dialog box appears.

2 From the **Configuration** drop-down list, select **Static**.

3 Select the **Configure interfaces in Drop-In mode** check box.



4 In the **IP Address** text box, type the Firebox IP address. In the **Default Gateway** text box, type the default gateway for the Firebox interfaces.
When you type an IP address, type all the numbers and the dots. Do not use the TAB or arrow key.

Note

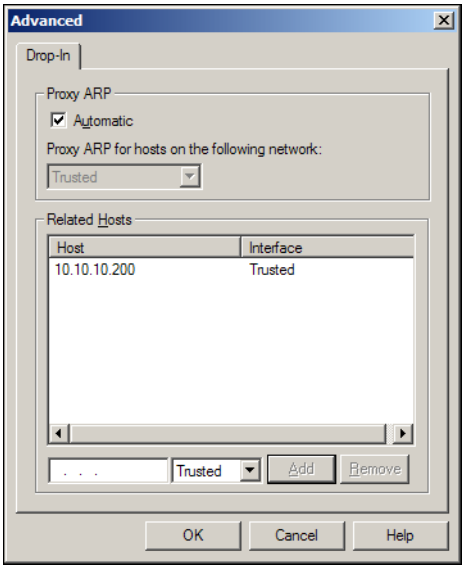
You can not use drop-in configuration if your ISP uses DHCP or PPPoE to give the Firebox its IP address.

Using proxy ARP

If you use the drop-in configuration mode, the Firebox uses proxy ARP. With proxy ARP, the Firebox replies to all ARP requests from the external network for computers on your trusted and optional networks. This helps to hide those computers from the Internet and to protect them from hackers.

From the **Network Configuration** dialog box, click **Properties**.

The Advanced dialog box appears. It shows the Drop-In tab.



Proxy ARP can operate as automatic or not automatic:

Using the Automatic check box

WatchGuard recommends that you select the **Automatic** check box. When you select the **Automatic** check box, the drop-in configuration mode automatically uses proxy ARP between the external network and the trusted and optional networks. The Firebox will do proxy ARP for any host on any interface if the host has an IP address in the drop-in network. This is the default setting for the drop-in configuration.

When the Automatic box is selected, you can move a computer from one interface to another only if you clear the ARP cache on that computer. To clear the ARP cache on a Windows computer, type the following at a command prompt:

```
arp -d *
```

Clearing the Automatic check box

You can clear the **Automatic** box to require all computers to be on one specified Firebox interface unless you list them as **Related Hosts** for that interface. If you clear the **Automatic** check box, do the following:

1 Use the **Proxy ARP for hosts on the following network** box to specify the Firebox interface that has the most computers in the drop-in network.
The Firebox expects that any computer in the drop-in network is on this interface.

2 Use the **Related Host** box to list computers in the drop-in network that can be on a different Firebox interface.

To list a Related Host:

1 Type the IP address of the host in the small text box at the bottom.

2 From the drop-down list at the bottom of the **Drop-In** tab, select the interface that the host is on.

3 Click **Add**.

4 Repeat steps 1 through 3 to add computers to other interfaces.

To remove a Related Host:

1 Select the Related Host in the large box.

2 Click **Remove**.

Note

Proxy ARP applies only to the drop-in configuration mode. Proxy ARP applies only to computers in the drop-in network.

Proxy ARP does not apply to routed mode configurations. Proxy ARP does not apply to the computers on a Secondary Network.

Setting the addresses in routed mode

In a routed configuration, you install the Firebox with different logical networks and network addresses on its interfaces. The public servers behind the Firebox usually use private (non-routable) IP addresses. If the computers behind the Firebox use private IP addresses, the Firebox uses network address translation (static NAT) to route traffic from the external network to the public servers.

You can also use the routed mode if you have different public (routable) IP address ranges behind the Firebox. If you use the routed mode, the interfaces must use different IP addresses. The Firebox interface IP addresses also must be on different subnets.

For example, you can not use 192.168.1.1/16 on one Firebox interlace and 192.168.2.1/16 on another Firebox interface. The /16 give a subnet mask of 255.255.0.0. This makes those two IP addresses the same subnet.

A minimum of two interfaces must have configured IP addresses. To use the Policy Manager to set the Firebox in routed configuration mode:

1 Click **Network** > **Configuration**.
The Network Configuration dialog box appears. The Interfaces tab displays.

2 If necessary, clear the **Configure interfaces in Drop-in mode** check box.

3 If your ISP uses DHCP or PPPoE to assign your IP address, select that option from the **Configuration** drop-down list.

4 If you have a static IP address from your ISP, select **Static** from the Configuration drop-down list. Type the static IP address you get from the ISP, and type the default gateway.

5 For each interface, type the IP address in slash notation.
When you type an IP address, type all the numbers and the dots. Do not use the TAB or arrow key.

Configuring the external interface

The Firebox can get a dynamic IP address for the external interface with Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE). Your ISP can also use DHCP or PPPoE to give the Firebox a static IP address. See “Using a static DHCP or static PPPoE address” on page 59 if your ISP gives you a static IP address and uses DHCP or PPPoE to give you that address. With DHCP, the Firebox uses a DHCP server which is controlled by your Internet Service Provider (ISP) to get an IP address, gateway, and subnet mask. With PPPoE, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. This connection automatically configures your IP address, gateway, and subnet mask. If you use DHCP or PPPoE for the external interface, you must set the Firebox to use the routed configuration mode.

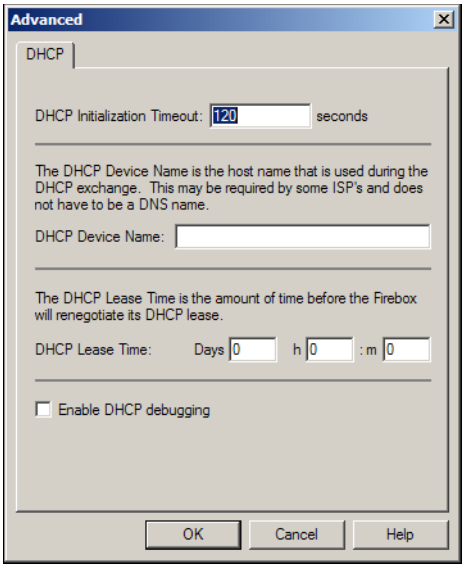
For more information about DHCP and PPPoE, refer to“Setting the external interface for DHCP” on page 58.

Setting the external interface for DHCP

1 Click **Network** > **Configuration**.
The Network Configuration dialog box appears.

2 From the **Configuration** drop-down list, select **DHCP**.

3 Click **Properties** to configure DHCP parameters.
Your ISP can tell you if it is necessary to change the time-out or device name values



Setting the external interface for PPPoE

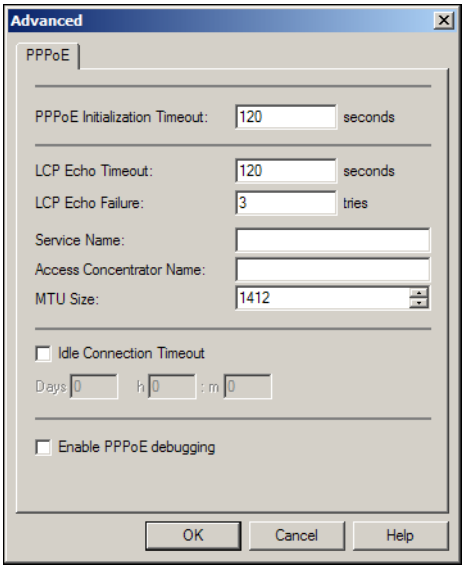
1 Click **Network** > **Configuration**.
The Network Configuration dialog box appears.

2 From the Configuration drop-down list, select **PPPoE**.

3 Type the **PPP User Name** and **PPP Password**. You must type the password two times.

4 Click **Properties** to configure PPPoE parameters.
Your ISP can tell you if it is necessary to change the time-out or LCP values. Your ISP can also give you the Service Name and Access Concentrator Name values to use if the ISP requires them. If you have problems with PPPoE

negotiations, you can change MTU size. Ask your ISP for a recommended MTU size. Usually the MTU value does not have to be changed.



Note

When you select the Enable PPPoE debugging check box, the Firebox sends a large volume of log messages to the log host. Do not use this feature unless you have problems with your connection and aid from Technical Support is necessary.

Using a static DHCP or static PPPoE address

With DHCP and PPPoE, usually the IP addresses that the ISP gives to customers can change. Some ISPs give you a static DHCP or PPPoE address. A static IP address can help you to configure device to device network traffic. For example, you must have a static IP address to use MUVPN and RUVPN with PPTP. To configure a static DHCP address or a static PPPoE address with the Policy Manager:

1 Click **Setup** > **Network Configuration**. Click the **Interfaces** tab.

2 From the **Configuration** drop-down list, select DHCP or PPPoE.

3 Click **Use the following IP address**. Type the static IP address.

Adding external IP aliases

The Firebox can receive traffic from the Internet and send it to a host behind the Firebox. The Firebox can use its own external IP address to receive this traffic, or it can receive traffic using another IP address that you get from the ISP. You add an **Alias** IP address to the Firebox external interface when these two things happen:

- The Firebox receives traffic on an IP address that is not the external interface IP address, **and**
- The Firebox sends this traffic to a different IP address behind the Firebox.

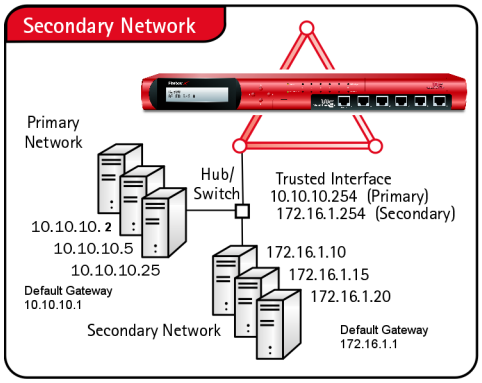
Note

Only use an alias for static NAT. Do not use an alias for 1-to-1 NAT. If you add an alias for 1-to-1 NAT, the 1-to-1 NAT will not operate. For more information see “Using 1-to-1 NAT” on page 90.

You can use the **Aliases** button on the **Network Configuration** dialog box to add Alias IP addresses to the Firebox external interface. You use the alias IP address when you set a service to use static NAT. You can also add the alias IP address when you set a service for static NAT from the **Add Static NAT** box. For more information, see “Setting static NAT for a service” on page 89.

Adding Secondary Networks

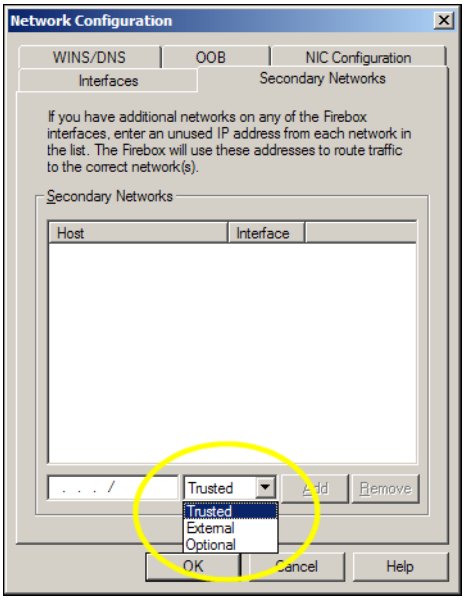
When you add a secondary network to a Firebox interface, you indicate that there is another logical network on that interface. To add a secondary network to a Firebox interface, you add another IP address and subnet mask to that Firebox interface. The IP address you use for the Secondary Network IP address must not be assigned to any other host on the secondary network. This IP address is the default gateway for all the computers on the secondary network and tells the Firebox that there is more than one network on the Firebox interface.



To use the Policy Manager to configure a secondary network:

1 Click **Network** > **Configuration**.
The Network Configuration dialog box appears.

2 Click the **Secondary Networks** tab.
The Secondary Networks tab appears.



3 Use the drop-down list in the lower part of the dialog box to select the interface to which the secondary network connects.

4 Type an IP address from the secondary network in the text box adjacent to the drop-down list. Use slash notation to show the subnet mask. Because this IP address is assigned to the Firebox interface, it must not be assigned to any other computer on the secondary network.
When you type an IP addresses, type all the numbers, the dots, and the slash. Do not use the TAB or arrow key. For more information on how to type the IP address, refer to "Enter the IP addresses" on page 38.

Note

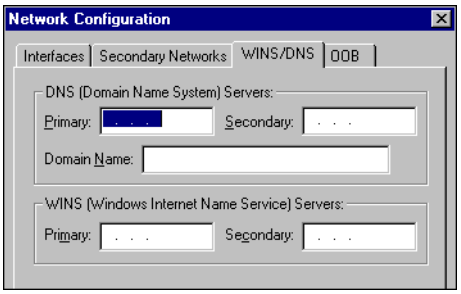
Be careful to add secondary network addresses correctly. The Policy Manager does not tell you if the address is correct. WatchGuard recommends that you do not enter a subnet on one interface that is a component of a larger network on a different interface. If you do this, spoofing can occur and the network can not operate correctly.

Adding WINS and DNS Server Addresses

A number of the features of the Firebox share the same Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. These features include DHCP, Mobile User VPN with IPSec, and Remote User VPN with PPTP.

If you have an internal private DNS server, make sure that you use your private DNS server for DHCP and Remote User VPN. If you also use external DNS servers, make the internal DNS server the Primary DNS server. If you do not have a private internal DNS server, list the DNS servers that your ISP provides. From Policy Manager:

1 Click **Network** > **Configuration**. Click the **WINS/DNS** tab.
The WINS/DNS tab appears.



2 Type the primary addresses and secondary addresses for the WINS and DNS servers. If necessary, type a domain name for the DNS server.

Configuring the Firebox as a DHCP Server

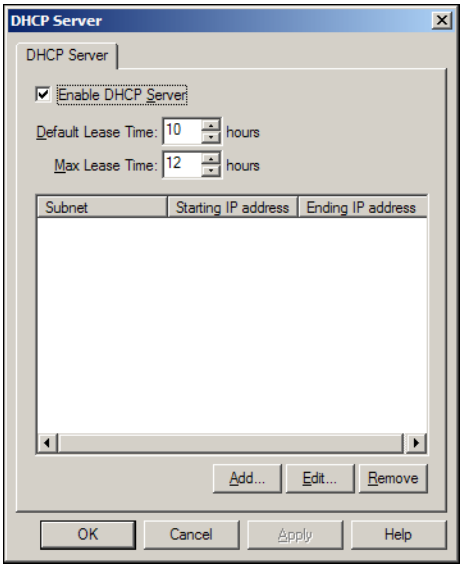
Dynamic Host Configuration Protocol (DHCP) is an Internet Protocol that makes it easier to control a large network. A computer you configure as the DHCP server automatically gives IP addresses to the computers on your network. You set the range of addresses. If you have a configured DHCP server on your network, you can use it with the Firebox. Or, you can configure the Firebox as a DHCP server for networks behind the firewall.

Note

If you have a large network with a domain controller on it, WatchGuard recommends that you configure the domain controller as the DVCP server.

One parameter that you set for a DHCP server is the lease time. This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the time is near its limit, the client transmits data to the DHCP server to get a new lease.

1 From Policy Manager, click **Network** > **DHCP Server**.
The DHCP Server dialog box appears.



2 Select the **Enable DHCP Server** check box.

3 Use the value control to change the **Default Lease Time**.
You can set the lease time on the client. If you do not, the DHCP Server uses the Default Lease Time value.

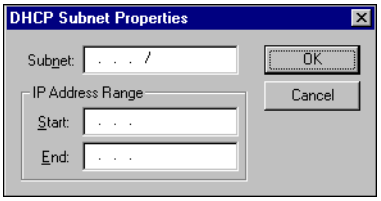
4 Use the value control to change the **Maximum Lease Time**.
Again, you can set the lease time on the client. If the time set on the client is larger than the Maximum Lease Time, the DHCP Server uses the value you set here.

Adding a subnet

The DHCP server assigns IP addresses to DHCP clients from a range you set. A subnet is a group of IP addresses you add to the DHCP server. For example, if you add a subnet of 10.1.1.10 to 10.1.1.19, the DHCP server has 10 addresses to give its clients.

1 From Policy Manager, click **Network** > **DHCP Server.**

2 Click **Add**.
The DHCP Subnet Properties dialog box appears.



3 In the **Subnet** text box, type the IP address and netmask of the subnet, for example, 10.1.1.0/24.

4 In the **Start** text box, type the first IP address in the range. In the **End** text box, type the last IP address in the range. The Firebox gives IP addresses only from this range to DHCP clients.

5 Click **OK**.

Changing a subnet

You can change a DHCP subnet. From Policy Manager:

1 Click **Network** > **DHCP Server**.

2 Click the subnet you want to change. Click **Edit**.
The **DHCP Subnet Properties** dialog box appears.

3 Type in new values for the **Subnet**, **Start**, or **End** text boxes. Click **OK**.

Removing a subnet

You can remove a DHCP subnet. From Policy Manager:

1 Click **Network** >**DHCP Server**.

2 Click the subnet you want to remove. Click **Remove**.

3 Click **OK**.

When you change or remove a DHCP subnet, this can cause problems. When the Firebox gives a DHCP client a different IP address, some devices or software applications can possibly not operate properly. This occurs only after the client gets a new IP address from the DHCP server.

Adding Basic Services to Policy Manager

To create an operational configuration file without using the Quick Setup Wizard, you must add four services to your security policy. This gives your Firebox some basic functionality. We recommend that you add:

- **WatchGuard** — Allows you to connect to the Firebox from the management station. You must have this service to monitor and configure the Firebox.

Note

The WatchGuard service is very important. If you do not include it in your configuration or if you configure it incorrectly, it prevents you from managing the Firebox.

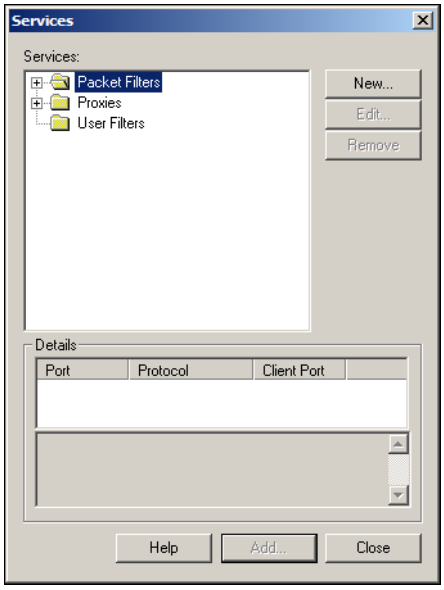
- **Ping** — Allows you to ping the Firebox and to ping computers on the external interfaces. This is an important tool to troubleshoot your network connections.
- **FTP** — Allows you to download files with File Transfer Protocol.

- **Outgoing** — Allows all network traffic which starts from the trusted or optional networks out to the external network. This lets your users send traffic to the Internet while you configure your security policy.

At this time, do not change the default configuration for these basic services. The default configuration lets all traffic out but does not let traffic in. You can make changes to these services in Policy Manager after you have confirmed that the Firebox operates correctly with your basic configuration file. For more information, refer to "Adding and Configuring Services" on page 41.

1 From Policy Manager, click **Edit** > **Add Service**.

Or click the Add Services icon on the Policy Manager toolbar. This icon is shown on the left. The Services dialog box appears.



2 Click the plus (+) sign on the left side of the **Packet Filters** folders to expand it.
A list of configured filters appears.

3 Below **Packet Filters**, click **WatchGuard**.

4 At the bottom of the dialog box, click **Add**.

5 Click **OK** in the **Add Service** dialog box.

6 Click **OK** to close the **Properties** dialog box.

7 Do steps 3–6 again for the **Ping**, **FTP**, and **Outgoing** services.

Configuring Routes

A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two networks. A packet can go through a number of network points with routers before it gets to its destination.

The Firebox lets you create static routes to send traffic from its interfaces to a router. The router can then send the traffic to the applicable destination in the specified route.

For more information about network routes and routers, refer to:

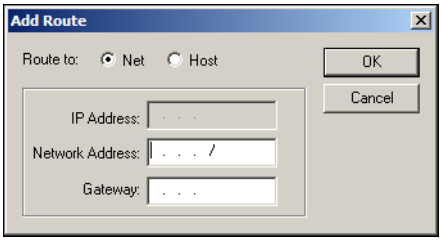
www.watchguard.com/support/AdvancedFaqs/general_routers.asp

Adding a network route

Add a **network** route if you have a full network behind a router on your local network. Type the network IP address, with slash notation.

1 From Policy Manager, click **Network** > **Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears.

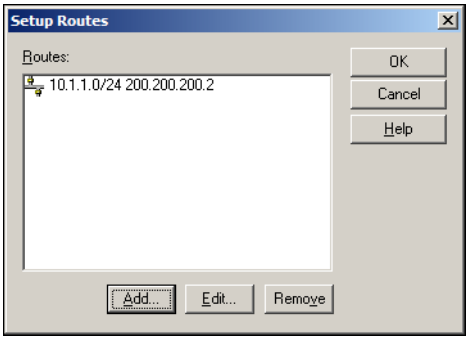


3 To the right of **Route to**, click **Net**.

4 In the **Network Address** text box, type the network IP address. Use slash notation.
For example, type 10.10.1.0/24. This is the 10.0.1.0 network with subnet mask 255.255.255.0.

5 In the **Gateway** text box, type the IP address of the router.
Make sure that you enter an IP address that is on one of the networks that you find on a Firebox interface. The Gateway for the route can not be in the destination network.

6 Click **OK** to close the Add Route dialog box.
The Setup Routes dialog box shows the configured network route.



7 Click **OK** again to close the Setup Routes dialog box.

Adding a host route

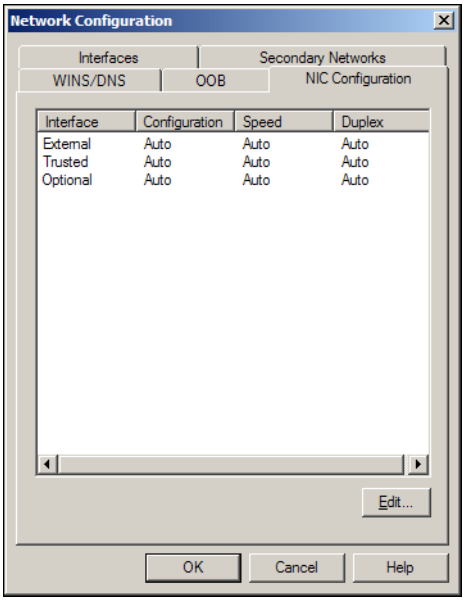
Add a **host** route if there is only one host behind the router or you only want traffic to go to one host. Type the IP address of that specified host, with no slash notation. From Policy Manager:

1 Click **Network** > **Routes**.
The Setup Routes dialog box appears.
2 Click **Add**.
The Add Route dialog box appears.
3 To the right of **Route to**, click **Host**.
4 In the Network Address text box, type the network IP address. Use slash notation.
5 In the **Gateway** text box, type the IP address of the router.
Make sure that you enter an IP address that is in one of the networks that you find on a Firebox interface.
6 Click **OK** to close the Add Route dialog box.
The Setup Routes dialog box shows the configured host route.
7 Click **OK** against to close the Setup Routes dialog box.

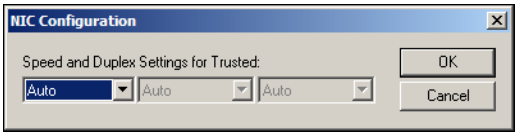
Firebox interface speed and duplex

You can set the speed and duplex properties for Firebox interfaces to automatic or manual configuration. WatchGuard recommends that you use automatic configuration because it operates with most network devices. Use manual when you must override the Firebox interface parameters to operate with other devices on your network.

1 Click **Network** > **Configuration**. Click the **NIC Configuration** tab.
The NIC Configuration tab appears.



2 Click the interface you want to change. Click **Edit**.



3 From the drop-down lists, select **Auto** or **Manual**. If you select **Manual**, select the speed and half-duplex or full-duplex.

4 Click **OK** to close the NIC Configuration dialog box. Click **OK** again to close the Network Configuration dialog box.

CHAPTER 7

Configuring Proxied Services

A packet filter examines each packet header. If the packet header information matches the rule criteria, then the firewall allows the packet. A proxy examines each packet header and the content of each packet. If the content does not match the rule criteria you set, the Firebox denies the packet.

A proxy operates at the application layer, while a packet filter operates at the network layer and transport layer. When you enable a proxy, the Firebox:

- Removes all the network data
- Examines the contents for RFC compliance and content type matches.
- Adds the network data again
- Sends the packet to its initial destination

A proxy uses more resources and bandwidth than a packet filter. But, a proxy can catch dangerous content types that a packet filter cannot.

For example, an e-mail proxy examines the header and the content of the SMTP packets. A software application in the content could be a virus. You can set the software applications and content types the e-mail proxy allows and which it denies. This is not possible with a packet filter.

To add or configure a proxy, refer to "Adding and Configuring Services," on page 41. For more information on proxies, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/proxy_main.asp

Protocol Anomaly Detection

Protocol anomaly detection (PAD) is a strong technology for the protection of your network. In network security, a protocol anomaly is data, content, or network traffic that is different from usual. It includes the network traffic that does not obey RFC requirements. As the network protocols are frequently fully specified, you can make a good model of the possible packets and record the packets that are different. You can also automatically add to the Blocked Sites list the source IP address of a computer that sends a packet with an anomaly.

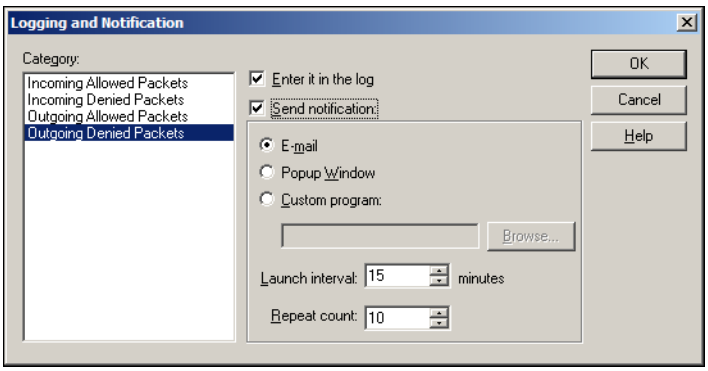
You can set the rules the Firebox uses to identify protocol anomalies. Protocol anomaly detection is available for the most frequently used traffic types such as: SMTP, FTP, HTTP, and DNS. Use a proxy to enable PAD.

Customizing Logging and Notification for Proxies

You can use the same procedure to customize the log and notification properties for a proxy as you do for a packet filter. To configure the log and notification properties for a proxy:

1 From the Properties dialog box in Policy Manager, click the **Incoming** tab.

2 Click Logging.
The Logging and Notification dialog box appears. :



3 Change the **log and notification** properties.

Configuring an SMTP Proxy Service

The SMTP Proxy protects you against dangerous content in e-mail messages. The proxy examines the **content type** and **content disposition** headers, and compares them with a user specified list of not approved content types. The proxy removes the not approved attachment from the e-mail message and sends it to the initial destination.

The proxy can also set a limit on how large the message can be and the number of addresses in the e-mail. The Firebox then stops any e-mail that is larger than these limits.

The SMTP proxy also automatically removes some commands, for example, DEBUG.

These are the SMTP keywords that you can use:

DATA	EXPN
RCPT	HELP
MAIL	RSET
QUIT	ONEX
HELO	NOOP
VRFY	QSND

Here are the ESMTP keywords you can use:

AUTH	CHUNKING
BDAT	EHLO
BINARYMIME	ETRN
8BITMIME	SIZE

For more information on the SMTP proxy, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/proxy_smtp.asp

Configuring Incoming SMTP Proxy

Use the **Incoming SMTP Proxy** dialog box to set the incoming properties of the SMTP Proxy. You must have an SMTP Proxy icon in the Services Arena. For information on how to add a service, refer to "Adding and Configuring Services," on page 41.

1 From the Services Arena of the Policy Manager, double-click the SMTP Proxy icon to open **SMTP Properties**.

2 Click the **Properties** tab.

3 Click **Incoming**.

4 Change the properties on the **General** tab.
To see the function of each control, right-click the control, and then select What's This?

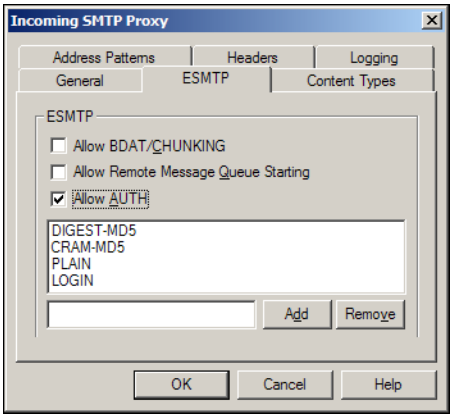
Configuring ESMTP

ESMTP (Extended Simple Mail Transfer Protocol) gives an extension to SMTP for enhanced delivery methods. On the ESMTP tab of the Incoming SMTP Proxy you can give ESMTP extensions (keywords) and AUTH types. The AUTH types give the SMTP server different authentication methods to use.

1 From the Incoming SMTP Proxy Properties dialog box, click the **ESMTP** tab.
The ESTMP information appears.

2 Select the check boxes to enable the necessary extensions.

3 Type the AUTH types in the text box. Click **Add**.
The proxy operates with all the AUTH types. The default AUTH types are DIGEST-MD5, CRAM-MD5, PLAIN, and LOGIN. Do not type ESMTP keywords in this text box. It is only for AUTH types.



Blocking e-mail attachments

There are two methods you can use to deny e-mail attachments:

- Deny specified file name patterns.
- Only let safe content types through

You can use the two methods at the same time. File pattern matches have higher precedence.

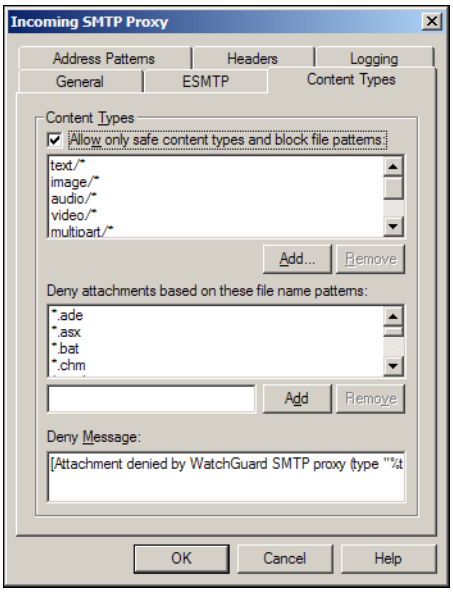
Allowing safe content types

Multipurpose Internet Mail Extensions (MIME) give the parameters for how e-mail or HTML send audio, video, and graphics content. The MIME format attaches a header to the content. The header identifies the multimedia content type that is in an e-mail or on a Web site.

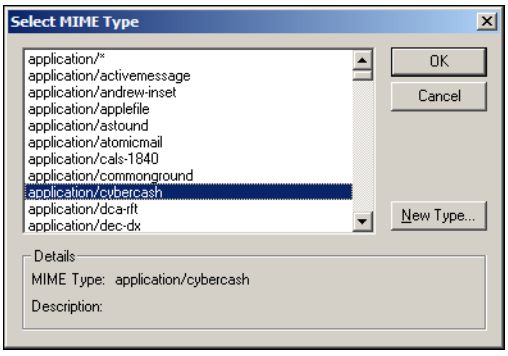
For example, a MIME type of "application/zip" in an e-mail message shows that the e-mail contains a Zip file. The Firebox can read the MIME header of each incoming e-mail, remove specified MIME types, and let others through. You set the types of attachments that are let through and the ones that are denied in the HTTP and SMTP Proxies of the Firebox.

1 From the Incoming SMTP Proxy Properties dialog box, click the **Content Types** tab.

2 Select the **Allow only safe content types and block file patterns** check box to block specified file name patterns in e-mail attachments.



3 Click the top **Add** button to see the pre-configured content types.
The Select MIME Type dialog box appears.



4 Select a MIME type. Use the CTRL key to select more than one entry. Click **OK**.

5 To add a new MIME type, click **New Type**. Type the MIME type and a description that will identify the MIME type in a list. Click **OK**.
The new MIME type appears at the bottom of the Content Types drop-down list. Do this for each content type. For a list of MIME content types, refer to the Reference Guide.

You can use the special characters as follows:

To allow content types

An asterisk (*) matches all the strings, including an empty string.

To deny file name patterns:

An asterisk (*) matches all the strings, including an empty string.
A question mark (?) matches a single character.

Denying attachments based on file name patterns

The **Content Types** tab includes a list of file name patterns that the Firebox denies, if they appear in e-mail attachments. To add a file name pattern to the list, type a new pattern in the text box on the left side of the **Add button**. Click **Add**.

Note that if a specified attachment is denied, protocol anomaly detection (PAD) rules do not automatically start. You must specially add the content type to PAD rules, refer to "Configuring Incoming SMTP Proxy" on page 71.

Specifying a denied message

In the **Content Types** tab, you can type a message to show when a content type is denied. This message shows to the recipient only and not the sender. A default message appears.

Use %t to add the content type to the message.

Use %f to add the file name pattern to the message.

Adding address patterns

You can add an address pattern to set the e-mail senders that are allowed or denied.

1 From **Incoming SMTP Proxy Properties**, click the **Address Patterns** tab.
2 From the **Category** drop-down list, select a category.
3 Type the address pattern in the text box on the left side of the **Add** button.
4 Click **Add**.
The address pattern appears at the bottom of the pattern list.

Protecting mail servers against relaying

A hacker or spammer can try to use an open relay to send e-mail from your servers. A good mail server configuration can prevent an open relay attack.

To increase the protection from e-mail relay, change the SMTP Proxy configuration to only let an address through from your domain.

1 From **Incoming SMTP Proxy Properties**, click the **Address Patterns** tab.
2 From the **Category** drop-down list, select **Allowed To.**
3 In the text box on the left side of the **Add** button, type your domain.
4 Click **Add**.
5 Save the new configuration to the Firebox.

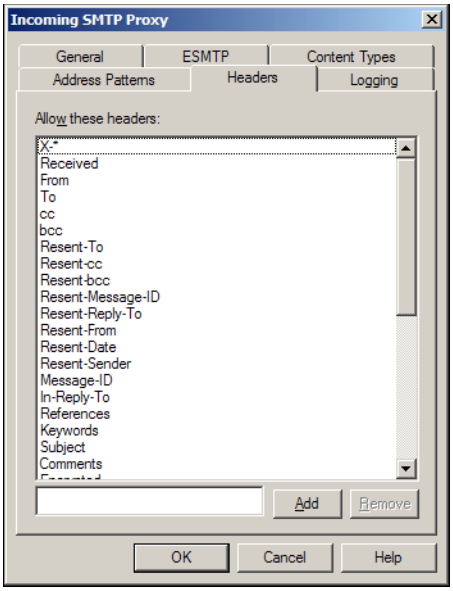
Note

If your external users send e-mail through your server, they can only send e-mail to your domain.

Select headers to allow

The Firebox gives its approval to specified headers by default. There is a list on the **Headers** tab of **Incoming SMTP Proxy Properties**. You can add more headers to this list, or remove the headers from the list.

1 From **Incoming SMTP Proxy Properties**, click the **Headers** tab.
The Headers information appears.



2 To add a new header, type the header name in the box on the left side of the **Add** button. Click **Add**.
The new header appears at the bottom of the header list.

3 To remove a header, select the header name in header list. Click **Remove**.

Specifying logging for the SMTP proxy

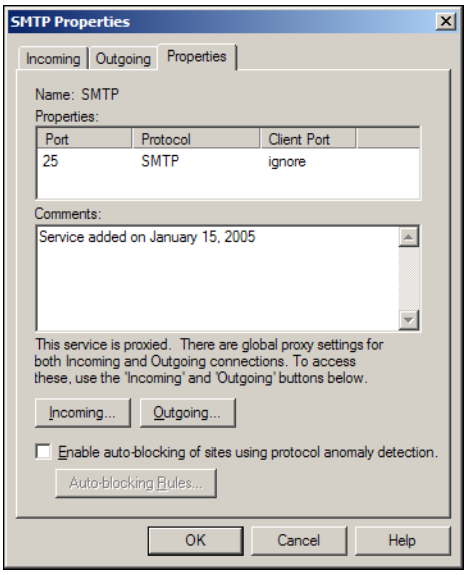
On the **Logging** tab, select to log:

- Unknown headers that the proxy filters.
- Unknown ESMTP extensions that the proxy filters.
- Accounting and auditing information.

Enabling protocol anomaly detection for SMTP

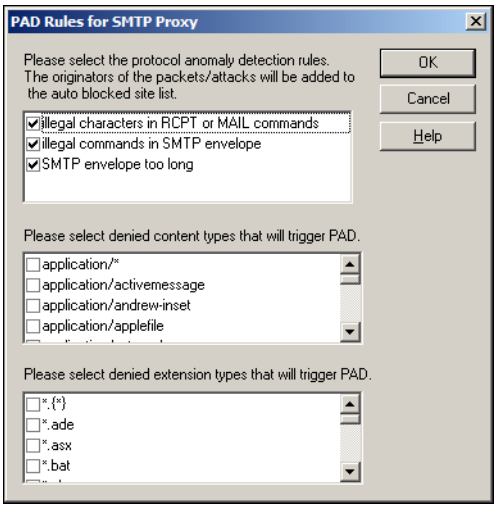
For more information on PAD, refer to “Protocol Anomaly Detection” on page 69.

1 From **SMTP Properties**, click the **Properties** tab.
The SMTP Properties dialog box appears.



2 Select the **Enable auto-blocking of sites using protocol anomaly detection** check box.

3 To set the rules for PAD, click **Auto-blocking Rules**.
The PAD Rules dialog box for SMTP Proxy appears.



4 In the top box, select the rules. When a site sends a packet that matches the rules, the Firebox automatically adds the site to the auto-blocked sites list.

5 The box that follows has the denied content types that are in the **Content Types** tab. Refer to “Allowing safe content types” on page 72.
PAD rules start with none of these content types enabled by default. To enable PAD for these content types, select the adjacent check box.
To select or erase a group of content types one after the other, select the first type, press and hold the Shift key and select the last type. To select or erase different content types as a group, press CTRL and select each type that is necessary.

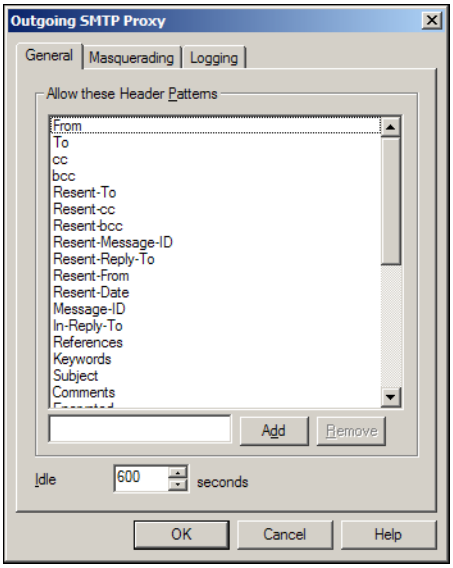
6 The box that follows has the list of the denied extension types that are listed on the **Content Types** tab. Refer to "Allowing safe content types" on page 72. PAD rules start with none of these extension types enabled by default. To enable PAD for these extension types, select the adjacent check box.

Configuring the Outgoing SMTP Proxy

Use **Outgoing SMTP Proxy** to set the properties for outgoing traffic. To do this, you must have an icon for the SMTP Proxy service in Services Arena.

1 Double-click the SMTP proxy icon to open the **Properties** dialog box. Click the **Properties** tab.

2 Click **Outgoing**.
The Outgoing SMTP Proxy dialog box appears.

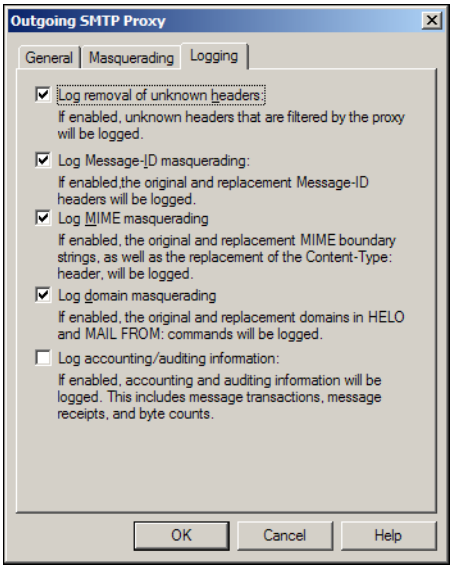


3 To add a new header pattern, type the pattern name in the box on the left side of the **Add** button. Click **Add**.

4 To remove a header from the pattern list, select header pattern. Click **Remove**.

5 In the **Idle** text box, type a time-out value in seconds.

6 Click the **Logging** tab to change the log properties. The options can help you to troubleshoot problems with your e-mail security.


Outgoing SMTP Proxy
General
Masquerading
Logging
Log removal of unknown headers:
If enabled, unknown headers that are filtered by the proxy will be logged.
Log Message-ID masquerading:
If enabled,the original and replacement Message-ID headers will be logged.
Log MIME masquerading
If enabled, the original and replacement MIME boundary strings, as well as the replacement of the Content-Type: header, will be logged.
Log domain masquerading
If enabled, the original and replacement domains in HELO and MAIL FROM: commands will be logged.
Log accounting/auditing information:
If enabled, accounting and auditing information will be logged. This includes message transactions, message receipts, and byte counts.
OK
Cancel
Help

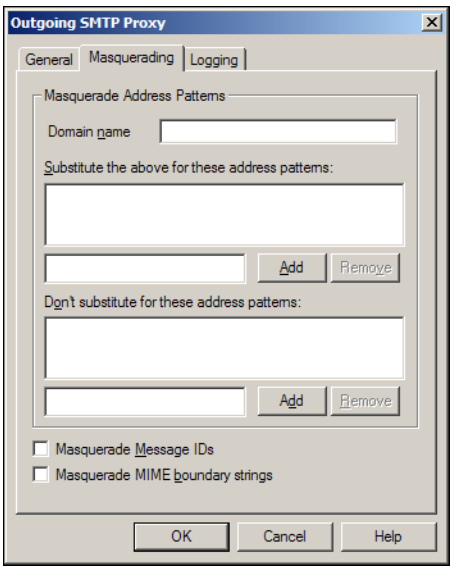
Note

If you send a large volume of e-mail, set outgoing to Disabled. This is a filter for outgoing e-mail that makes less work for the Firebox.

Add masquerading options

SMTP masquerading changes an address pattern behind the firewall into a public address. For example, the internal address pattern can be `inside.salesdept.bigcompany.com`, which becomes the public address `bigcompany.com`.

1 Click the **Masquerading** tab.
The SMTP masquerading information appears.



2 In the **Domain Name** text box, type the domain name.
This is the external name.

3 In the **Substitute the above for these address patterns** text box (on the left side of the **Add** button), type the address patterns that are behind your firewall. These will be replaced by the external domain name. Click **Add**.

4 In the **Don't Substitute for these address patterns** text box (on the left side of the **Add** button), type the address patterns that will appear "as is" external to the firewall. Click **Add**.

5 Select the **Masquerade Message IDs** check box to change the message-ID. The Message-ID and Resent-Message-ID in the header changes to a new ID. This has an encoded version of the initial ID, time, and domain name.

6 Select the **Masquerade MIME boundary strings** check box to change the MIME boundary strings in the messages and attachments. The firewall then changes them to a string that does not show internal host names or other information that can identify the sender.

Configuring An FTP Proxy Service

The FTP Proxy enables you to transmit data to and from a computer on a different network. You can look at the directories and copy data. If not set up correctly, the FTP Proxy can let a hacker have access to your network and important information that includes your passwords and configuration data.

Outbound FTP traffic can also be dangerous. It enables the users on your network to copy data to a location behind your firewall. Thus, it is important to set a limit on the FTP Proxy.

You must try to isolate the incoming FTP servers to one host on your optional interface or on one of the less trusted interfaces. Make sure that you also protect your trusted network from FTP requests from other networks. The FTP Proxy has special features that give more control for the traffic that goes through your firewall.

For more information about the FTP Proxy, refer to the FAQ:

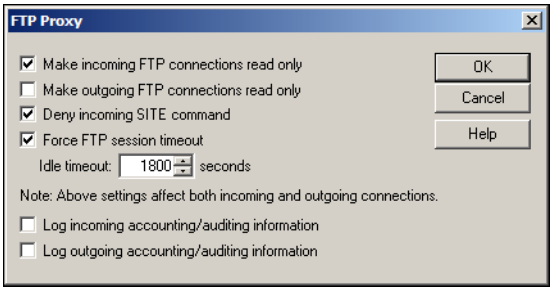
www.watchguard.com/support/advancedfaqs/proxy_ftp.asp

For troubleshooting information for the FTP proxy, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/proxy_ftptrouble.asp

1 From Policy Manager, click the **Add Service** button. Expand the Proxy services and double-click the FTP Proxy icon.

2 Click the **Properties** tab. Click **Settings**.
The Settings information appears.



3 Select the necessary FTP Proxy properties.
To see the function of each control, right-click it, and then select What's This?
Note that the **Make Incoming FTP Connections Read only** check box is selected by default. You must clear this check box to accept files.

4 Click **OK**.

Enabling protocol anomaly detection for FTP

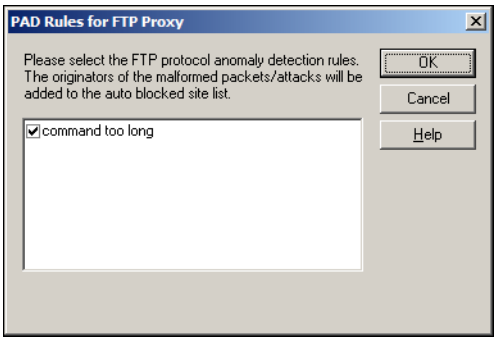
For a description of PAD, refer to "Protocol Anomaly Detection" on page 69.

From **FTP Properties**:

1 Click the **Properties** tab.

2 Select the **Enable auto-blocking of sites using protocol anomaly detection** check box.

3 To set PAD rules, click the **Auto-blocking Rules** button.
The PAD Rules dialog box for FTP Proxy appears.


PAD Rules for FTP Proxy
Please select the FTP protocol anomaly detection rules. The originators of the malformed packets/attacks will be added to the auto blocked site list.
OK
Cancel
Help
command too long

4 Select the rules to determine which hosts that send packets are automatically added to the auto-blocked sites list.

Selecting an HTTP Service

HTTP traffic can be a security risk. Set up public Web servers and allow incoming HTTP traffic only on the optional interface or on one of the less trusted interfaces of the Firebox. You can open outbound HTTP traffic from **Any to Any**.

Policy Manager for WFS has three types of HTTP service:

- **Proxied-HTTP** puts together two policies. It includes HTTP on port 80 and a rule that lets all outgoing TCP connections go through the Firebox. You can configure the log properties, safe content types, and WebBlocker from this service.
  This service does the routing of all the outgoing TCP connections, which includes non-HTTP traffic. Use the HTTP Proxy if you are not sure that this is best for you.
- **HTTP** is almost the same as Proxied-HTTP, but it controls the incoming and outgoing traffic on port 80.

Note

This "HTTP" service is not an HTTP caching proxy. An HTTP caching proxy is a different system that caches Web data.

- **Filtered-HTTP** puts together a pacekt filter for HTTP on port 80 with a rule that lets all the outgoing TCP connections go through.
  This packet filter service is much faster than Proxied-HTTP or HTTP, but it does not give the same protection. The features of Proxied-HTTP are not available for this service.

Adding a proxy service for HTTP

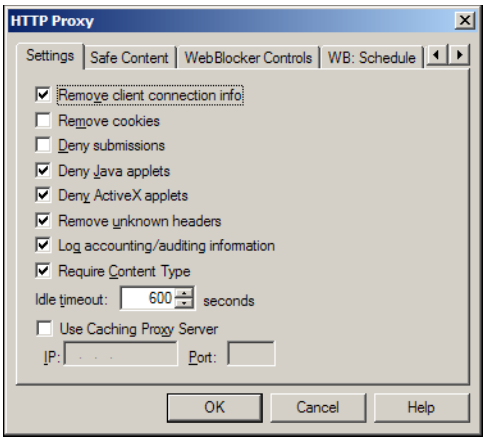
You can use the HTTP Proxy when you configure your Web traffic. You can put together the HTTP Proxy with an outgoing proxy service that you configure as **Any to Any**. The HTTP Proxy gives you easy control of Web traffic.

1 From Policy Manager, click the **Add Service** icon. Expand the **Proxies** folder, double-click **HTTP**, and then click **OK**.
The HTTP Properties appear. The default configuration is to deny incoming traffic and let outgoing traffic through from Any to Any.

2 From the **Incoming HTTP connections are** drop-down list, select **Enabled and Allowed**.

3 Configure the service as your business requires.
For example, you can configure the HTTP Proxy to let incoming traffic through from Any to the optional network or to a less trusted port. Click the **Add** button below the **To** list. In **Add Address**, add the **optional** Firebox group. Click **OK**.

4 Click the **Properties** tab. Click **Settings**.
The HTTP Proxy dialog box appears.



5 On the **Settings** tab, enable the necessary HTTP Proxy properties.

6 If you use the HTTP Proxy and also use WebBlocker, refer to Chapter 16, "Controlling Web Site Access."
To see the function of each control, right-click it, and then select What's This?

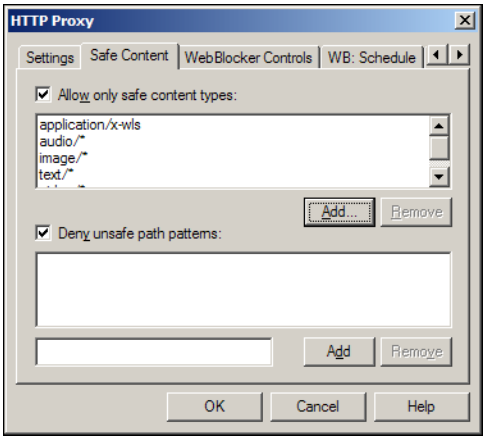
For more information on the HTTP proxy, refer to the FAQs at:

www.watchguard.com/support

Restricting content types for the HTTP proxy

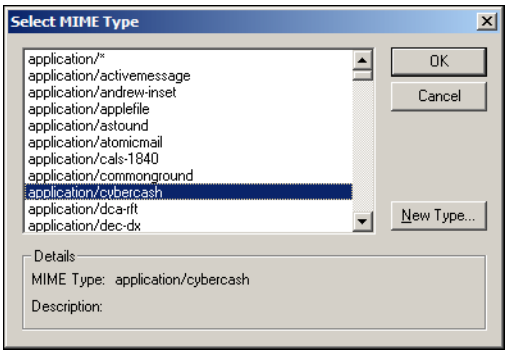
You can configure the HTTP Proxy to let only those MIME types through that you find are satisfactory security risks.

1 On the HTTP Proxy dialog box, select the **Safe Content** tab.



2 To put a limit on the content types that can go through the HTTP Proxy, select the **Allow only safe content types** check box.

3 To select the content types to let through, click the top **Add** button in the dialog box.
The Select MIME Type dialog box appears.



4 Select a MIME type. Click **OK**.

5 To make a new MIME type, click **New Type.** Type the MIME type and the function. Click **OK**.
The new type appears at the bottom of the Content Types drop-down list. Do this for each content type. For a list of MIME content types, refer to the Reference Guide.

6 To select path patterns that are not safe to block, type the path pattern on the left side of the **Add** button. Click **Add**.
You can set a filter on the path but not on the host name. For example, with the Web site www.testsite.com/login/here/index.html, you can add /login/ and /here/ or "*.html". You cannot add *testsite*.

Note

Zip files are denied when you block Java applets.

Configuring a caching proxy server

The HTTP Proxy on the Firebox does no content caching. The Firebox can use standard external caching proxy servers. Because your users can look at the same Web sites frequently, a caching proxy server

increases the traffic speed and decreases the traffic volume on the external Internet connections. All Firebox proxy and WebBlocker rules continue to have the same effect. The Firebox connection with a proxy server is the same as with a client.

To set up an external caching proxy server:

1 Configure an external proxy server, such as Microsoft Proxy Server 2.0 or Squid.

2 Open Policy Manager.

3 Double-click the icon for your HTTP proxy service.
This can be Proxy, HTTP, or Proxied-HTTP.

4 Click the **Properties** tab. Click the **Settings** button.

5 Select the **Use Caching Proxy Server** check box.

6 In the text boxes below the check box, type the IP address and TCP port of the caching proxy server. Click **OK**.

7 Save this configuration to the Firebox.

Configuring the DNS Proxy Service

With the Domain Name System (DNS) you can get access to a Web site with an easy "dot-com" name. DNS finds the Internet domain name (for example WatchGuard.com) and changes it to an IP address.

There is not one primary DNS, but there are many DNS lists on the Internet. You can make a DNS with Berkeley Internet Name Domain (BIND).

In the past, some versions of BIND were attacked and created a buffer overflow. This type of attack kills the server and can let an attacker get access to your network. Using the DNS Proxy in your WatchGuard System Manager configuration can protect you against new attacks as they are developed.

For more information on the DNS proxy, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/proxy_main.asp

Note

Use this proxy only if you have a DNS server for public use.

Adding the DNS Proxy Service

The DNS Proxy protects your network best when you use it for incoming traffic. You can also set up the DNS Proxy to send a log record for each denied packet (incoming or outgoing).

You can use the LogViewer to examine your log files. Look for the entries that show that there was a DNS attack. The entries show how much and from where you were attacked.

On the toolbar:

1 Click the **Add Services** icon.

2 Expand the **Proxies** folder.
A list of configured proxies appears.

3 Click **DNS-Proxy**. Click **Add**.
Add Service appears. You can change the name or the function of the DNS proxy.

4 Click **OK** to stop **Add Service**.
DNS-Proxy Properties appears.

5 Click the **Incoming** tab. From the **Incoming DNS-Proxy connections are** drop-down list, select **Enabled and Allowed**.

6 Click the **Outgoing** tab. From the **Outgoing DNS-Proxy connections are** drop-down list, select **Enabled and Allowed**.

7 Click **OK** and the **DNS Proxy Properties dialog box closes**. Click **Close**.
The DNS-Proxy icon appears in the Services Arena.

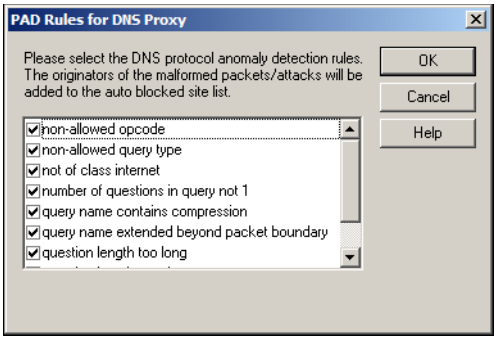
Enabling protocol anomaly detection for DNS

For a description of PAD, refer to "Protocol Anomaly Detection" on page 69.

1 In the **DNS Properties** dialog box, click the **Properties** tab.

2 Select the **Enable auto-blocking of sites using protocol anomaly detection** check box.

3 To set PAD rules, click the **Auto-blocking Rules** button.
The PAD Rules for DNS Proxy dialog box appears.


PAD Rules for DNS Proxy
Please select the DNS protocol anomaly detection rules. The originators of the malformed packets/attacks will be added to the auto blocked site list.
OK
Cancel
Help
non-allowed opcode
non-allowed query type
not of class internet
number of questions in query not 1
query name contains compression
query name extended beyond packet boundary
question length too long

4 By default, all rules are enabled. You can enable or remove the rules that find sites and automatically add them to the auto-blocked sites list.
To select or erase a group of rules one after the other, select the first rule, press Shift and select the last rule. Then select one of the rules between the two selections. To select or erase different rules as a group, press CTRL and select each rule that is necessary.

DNS file descriptor limit

The DNS Proxy can control only 256 Dynamic NAT connections at the same time. This limit is not usually a problem, but some Web sites can have slow name resolution and a high number of this log message:

```
dns-proxy[xx] dns_setup_connect_udp: Unable to create UDP socket for port: Invalid argument
```

You can put an end to this problem, as follows:

- Do not use dynamic NAT between your clients and your DNS server (most secure) or
- Do not use an outgoing DNS Proxy service and use a filtered DNS service.

CHAPTER 8

Configuring Network Address Translation

Network Address Translation (NAT) was originally designed as one of several solutions for organizations that could not obtain enough registered IP network numbers from Internet Address Registrars for their organization's growing population of hosts and networks.

NAT is generically used to describe any of the several forms of IP address and port translation. Its primary purposes are to stretch the number of computers able to work off of a publicly routable IP address, and to hide the private IP addresses of hosts on your LAN.

At its most basic level, NAT changes the address of a packet from one value to a different value. The type of NAT refers to how NAT changes the network address:

Dynamic NAT

Dynamic NAT is also known as IP masquerading. The Firebox can apply its public IP address to the outgoing packets for all connections or for specified services. This hides the real IP address of the computer that is the source of the packet from the external network.

Static NAT

Static NAT is also known as port forwarding. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a port on the external interface. Static NAT changes this address to an address and port behind the firewall. You must configure each service. You can use Static NAT for public services such as a Web server or FTP server.

1-to-1 NAT

The Firebox uses private and public IP ranges that you set for NAT. With 1:1 NAT, you bind a public address for each Web and other (DNS, mail) server to the private address you assigned to each server located on your trusted or optional networks. 1:1 NAT is useful for permitting public hosts access to internal servers.

The type of NAT you use depends upon your security policy. For more information on NAT, refer to the FAQ:

https://www.watchguard.com/support/advancedfaqs/nat_main.asp

Dynamic NAT

Dynamic NAT is the most frequently used type of NAT. It changes the source IP address of an outgoing connection to the public IP address of the Firebox. From the external network, you only see the external IP address of the Firebox on outgoing packets.

Many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for the internal hosts that use the Internet, because it can hide hosts on your network.

WatchGuard System Manager has two different ways to configure outgoing Dynamic NAT:

Simple Dynamic NAT
: With host aliases or host and network IP addresses, the Firebox applies NAT to each outgoing packet. This is the most frequently used type of NAT.

Service-based dynamic NAT
: You must configure each service for outgoing Dynamic NAT. Usually, you use this type of NAT only together with the drop-in mode of Firebox configuration.

Note

Computers that make an incoming connection on a VPN can connect to hosts by their correct private address.

Using Simple Dynamic NAT

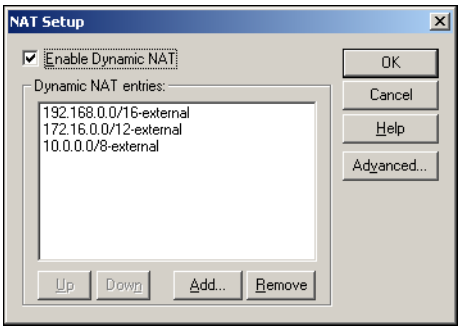
In most networks, the recommended security policy is to apply NAT to all outgoing packets. With **simple dynamic NAT** you can quickly set up a NAT policy for all of your network. For more information on this type of NAT, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/nat_howdynamicnat.asp

Enabling simple dynamic NAT

The default configuration of **simple dynamic NAT** enables dynamic NAT from all private IP addresses to the external network.

1 From Policy Manager, click **Setup** > **NAT**.
The NAT Setup dialog box appears.



2 Select the **Enable Dynamic NAT** check box.

The default entries are:

- 192.168.0.0/16 - external
- 172.16.0.0/12 - external

- 10.0.0.0/8 - external.

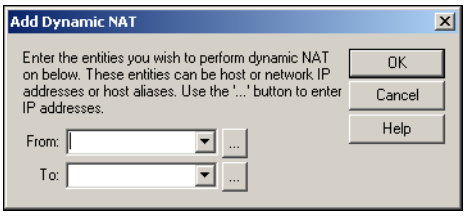
These are the private networks given by RFC 1918. TO enable dynamic NAT for private IP addresses other than these, you must add an entry for them.

Adding simple dynamic NAT entries

With default host aliases, the Firebox hides addresses from your trusted and optional networks.

For larger networks or networks with more services, you can have more entries in the **From** or **To** lists of hosts or host aliases. For example, a dynamic NAT entry "trusted_optional" would use NAT on all traffic routed from the trusted network to the optional network with the Firebox's optional IP address.

1 From the **NAT Setup** dialog box, click **Add**.


Add Dynamic NAT
Enter the entities you wish to perform dynamic NAT on below. These entities can be host or network IP addresses or host aliases. Use the '...' button to enter IP addresses.
OK
Cancel
Help
From:
To:

2 From the **From** drop-down list, select the source of the outgoing packets or type a network address.
For example, use the trusted host alias to enable NAT from the full trusted network. For more information on built-in Firebox aliases, refer to "Using Aliases" on page 93. For more information on how to add a user-defined host alias, refer to "Adding an alias" on page 94.

3 From the **To** drop-down list, select the destination of the outgoing packets.

4 To add a host or a network IP address, click the **...** button. From the drop-down list, select the address type. Type the IP address or the address range. You must type a network address in slash notation.
When you type an IP address, type all the numbers and the stops. Do not use the TAB or arrow key.

5 Click **OK**.
The new entry appears in the **Dynamic NAT Entries** list.

Reordering simple dynamic NAT entries

To change the sequence of the dynamic NAT entries, select the entry to change. Then click the **Up** or **Down** button.

You cannot change a dynamic NAT entry. To do this, You must erase the entry with the **Remove** button. Use the **Add** button to add the new entry.

Specifying simple dynamic NAT exceptions

You can set up ranges of addresses in dynamic NAT and make each address in that range a part of the NAT policy. With the **dynamic NAT exceptions** parameter you can remove some addresses from that policy.

1 From Policy Manager, click **Setup** ›**NAT**.

2 Click **Advanced**.
The Advanced NAT Settings dialog box appears.

3 Click the **Dynamic NAT Exceptions** tab.

4 Click **Add**.
The Add Exception dialog box appears.

5 In the **From** and **To** boxes, select the interface you want.
The alternatives dvcp_nets and dvcp_local_nets are aliases for VPN Manager and appear if you configure your Firebox as a DVCP client. dvcp_nets refers to networks at the other end of the VPN tunnel. dvcp_local_nets refers to networks behind the Firebox that you configure. Do not make dynamic NAT exceptions for these networks.

6 Click the button adjacent to the **From** box. Type the value of the host IP address, network IP address, or host range. Click **OK**.

7 Click **OK** to close the **Advanced NAT Settings** dialog box.

Note

You can configure Dynamic NAT exceptions on the two types of dynamic NAT. You must make dynamic NAT exceptions for each 1-to-1 NAT address if it is also configured by dynamic NAT.

Using Service-Based Dynamic NAT

With service-based dynamic NAT, you can set an outgoing dynamic NAT policy for each service. Use Service-based NAT to make exceptions to a simple dynamic NAT entry that applies to all connections.

For example, you have a network with simple NAT enabled from the trusted to the optional network. A web server on the optional network must not be masqueraded to the trusted network. To do this, you use service-based NAT. Add a service icon that lets Web connections through from the trusted to the optional Web server, and make NAT inactive. In this configuration, you make all Web connections with the correct source IP from the trusted network to the Web server. All other traffic from trusted to optional is masqueraded. You can also use service-based NAT as an alternative to simple dynamic NAT. You do not apply all NAT rules to all the outgoing packets, but you select the specified services to masquerade.

Enabling service-based dynamic NAT

To enable Service-based NAT you do not have to enable **simple dynamic NAT.** From Policy Manager:

1 Click **Setup** > **NAT**. Click **Advanced**.

2 Select the **Enable Service-Based NAT** check box.

3 Click **OK** to close the **Advanced NAT Settings** dialog box. Click **OK** to close the **NAT Setup** dialog box.

Configuring service-based dynamic NAT

By default, a service has the dynamic NAT properties you set for simple NAT. But, you can override this in the **Properties** dialog box of the service. You can select:

Use Default (Simple NAT)

Service-based NAT is not enabled for the service. The service uses the simple dynamic NAT rules that you configure in the **Dynamic NAT Entries** list. For more information, refer to "Adding simple dynamic NAT entries" on page 87.

Disable NAT

Makes dynamic NAT not active for the outgoing packets that use this service. Use this to not include a service in outgoing NAT.

Enable NAT

Enables service-based dynamic NAT for outgoing packets. This service overrides the simple dynamic NAT configuration.

From Policy Manager:

1 Double-click the service icon. Click **Outgoing**.

2 From the **Choose Dynamic NAT Setup** drop-down list, select **default** (simple dynamic NAT), **disable**, or **enable**. Click **OK**.

Configuring Service-Based Static NAT

For more information on static NAT, refer to the FAQs:

www.watchguard.com/support/advancedfaqs/nat_whenstatic.asp
www.watchguard.com/support/advancedfaqs/nat_outin.asp

Setting static NAT for a service

You must configure Static NAT for each service. Because of how static NAT operates, it is available only for services that use a specified port, which include TCP and UDP. A service that has an other protocol cannot use incoming static NAT. And the **NAT** button in the **Properties** dialog box of the service does not work. You also cannot use Static NAT with the **Any** service. Before you configure static NAT for a service, refer to the FAQ:

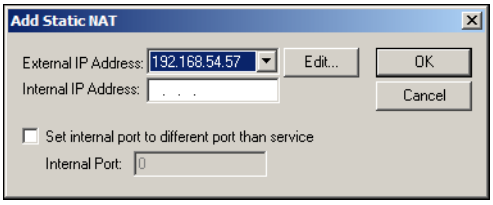
https://www.watchguard.com/support/advancedfaqs/nat_outin.asp

1 Double-click the service icon in the Services Arena.
The Properties dialog box of the service shows the Incoming tab.

2 From the **Incoming** drop-down list, select **Enabled and Allowed**.
To use static NAT, the service must let incoming traffic through.

3 Below the **To** list, click **Add**.
The Add Address dialog box appears.

4 Click **NAT**.
The Add Static NAT dialog box appears.



Note

Mail servers should generally use 1-to-1 NAT instead of static NAT. If not, e-mail problems can occur.

5 From the **External IP Address** drop-down list, select the "public" address to use for this service.

6 Type the internal IP address.
The internal IP address is the destination on the inside of the Firebox.

7 If necessary, select the **Set internal port to different port than service** check box.
You usually do not use this feature. It enables you to change the packet destination not only to a specified internal host but also to a different port. If you select the check box, type the different port number in the Internal Port text box.

8 Click **OK** to close the **Add Static NAT** dialog box.
The static NAT route appears in the Members and Addresses list.

9 Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **Properties** dialog box of the service.

Using 1-to-1 NAT

1-to-1 NAT uses a NAT policy that changes and routes all incoming and outgoing packets sent to one range of addresses to a different range of addresses. You can configure many different 1-to-1 NAT addresses.

You frequently use 1-to-1 NAT to route public IP addresses to internal servers. On those servers, you do not have to change the IP address. You can also use 1-to-1 NAT for VPN tunnels when the IP addresses of the remote network are the same as the local network. The local network addresses change to a range that is not the same as the remote addresses, and a VPN tunnel can connect.

For more information on 1-to-1 NAT, refer to the FAQ:

https://www.watchguard.com/support/advancedfaqs/nat_onetoone.asp

In each NAT policy you can configure four items:

- The interface
- The public IP address (NAT base)
- The internal IP address (real base)
- The number of hosts to apply NAT to.

You set a NAT policy in a "from" and "to" range of IP addresses. For example, in this policy:

```
210.199.6.1-192.168.69.1:254 (NAT base to real base range)
```

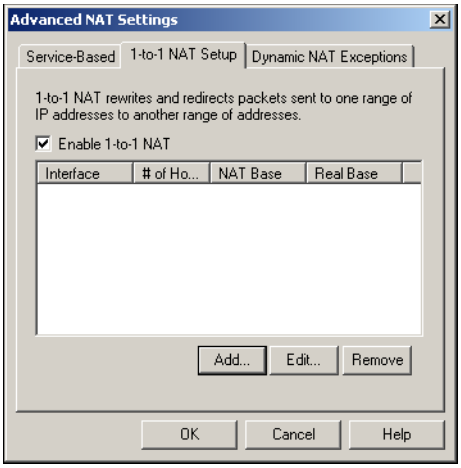
all the traffic that is sent to hosts between 210.199.6.1 and 210.199.6.254 change to the related IP address between 192.168.69.1 and 192.168.69.254.

There is a one-to-one address change from each NAT address to the destination (real) IP address: 210.199.6.0 becomes 192.168.69.0.

1 From Policy Manager, click **Setup** > **NAT**.

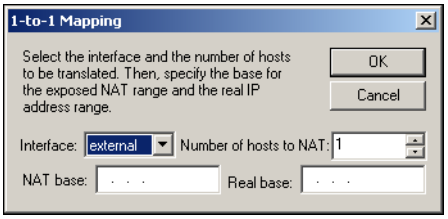
2 Click **Advanced**.
The Advanced NAT Settings dialog box appears.

3 Click the **1-to-1 NAT Setup** tab.



4 Select the **Enable 1-1 NAT** check box.

5 Click **Add**.
The 1-1 Mapping dialog box appears.


1-to-1 Mapping
Select the interface and the number of hosts to be translated. Then, specify the base for the exposed NAT range and the real IP address range.
OK
Cancel
Interface:
external
Number of hosts to NAT:
1
NAT base:
Real base:

6 Select the interface associated with the public (NAT base) IP address or addresses.

7 Type the number of hosts to route.

8 In the **NAT base** text box, type the address for the NAT range you can see externally.
This is usually the public IP address.

9 In the **Real base** text box, type the destination IP address range. Click **OK**.
This frequently is the IP address the server or client has.

10 Click the **Dynamic NAT Exceptions** tab.
You must make dynamic NAT exceptions for each internal address you use for 1-to-1 NAT. If not, the address changes with dynamic NAT as an alternative to 1-to-1 NAT.

11 Click **Add.**
The Add Exception dialog box appears.

12 In the **To** box, select the interface you want. This usually is the external interface.
The alternatives dvcp_nets and dvcp_local_nets are aliases for VPN Manager and appear if you configure your Firebox as a DVCP client. dvcp_nets refers to networks at the other end of the VPN tunnel. dvcp_local_nets refers to networks behind the Firebox that you configure. Do not make dynamic NAT exceptions for these networks.

13 Click the button adjacent to the **From** box. Type the IP address range you gave in step 9. Click **OK**.

14 Click **OK** to close the **Advanced NAT Settings** dialog box. Click **OK** to close the **NAT Setup** dialog box.

Proxies and NAT

The table that follows gives each proxy and the possible types of NAT.

	Simple dynamic	Static	Service-based	1-to-1
DNS	yes	yes	yes	yes
HTTP	yes	yes	yes	yes
SMTP	yes	yes	yes	yes
FTP	yes	yes	yes	yes
DCE-RPC	yes	no	no	no
H323	yes	no	no	no

CHAPTER 9

Creating Aliases and Implementing Authentication

An *alias* is a shortcut that identifies a group of hosts, networks, or users. When you use an alias, it can be easy to create a security policy.

With user authentication you can monitor a connection with a name and not as an IP address. The person authenticates with a user name and a password to get access to Internet tools, for example outgoing HTTP or outgoing FTP. The IP address or the computer that the person uses is not important. While the person is authenticated, all the connections that the person starts from that IP address also transmit the session name. This lets you monitor not only the computers from which the connections start, but also the person.

Note

The user name stays with the IP address. We do not recommend that you use user authentication with shared multi-user computers (Unix, Citrix, or NT terminal servers), because each shared server can only authenticate one user at a time.

The Firebox® allows you to create policies and groups with user names. A person can use more than one computer or IP address with the same user name. It is good to monitor by user name if you use the Dynamic Host Configuration Protocol (DHCP) because a computer can have more than one IP address in a week. It is also a good to monitor by user name in organizations where many different persons can use the same IP address in a day.

For more information on authentication, refer to the FAQs:

www.watchguard.com/support/advancedfaqs/auth_main.asp

Using Aliases

With an alias it is not necessary to know the host IP addresses, host ranges, or network IP addresses. An alias operates almost as an e-mail group name. It puts together the addresses and names into groups that are easy to identify. You can use an alias to quickly create filter rules. You cannot use an alias to configure the network.

WatchGuard automatically adds six aliases to the basic configuration:

Group	Function
firebox	The addresses for the three Firebox interfaces and related networks or device aliases
trusted	The hosts or networks that go through the physical trusted interface
optional	The hosts or networks that go through the physical optional interface
external	The hosts or networks that go through the physical external interface. Frequently, this is the Internet
dvcp_nets	The networks at the other end of a VPN tunnel
dvcp_local_nets	The networks behind the Firebox that you configure

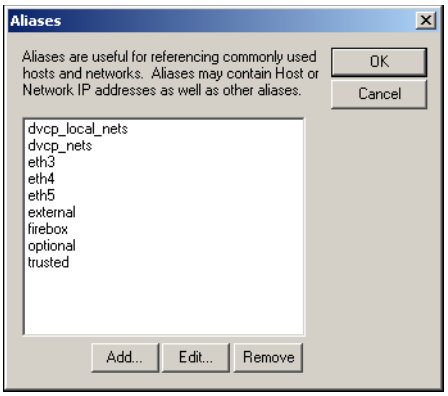
The optional Firebox X 3-Port Upgrade also adds the aliases eth3, eth4, and eth5.

A host alias overrides a Windows NT or RADIUS group with the same name.

Adding an alias

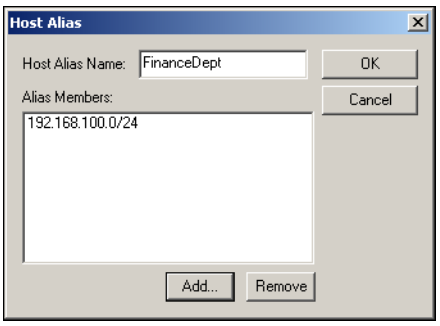
Use Policy Manager for WFS to add an alias.

1 From the Policy Manager, click **Setup** > **Aliases**.
The Aliases dialog box appears.

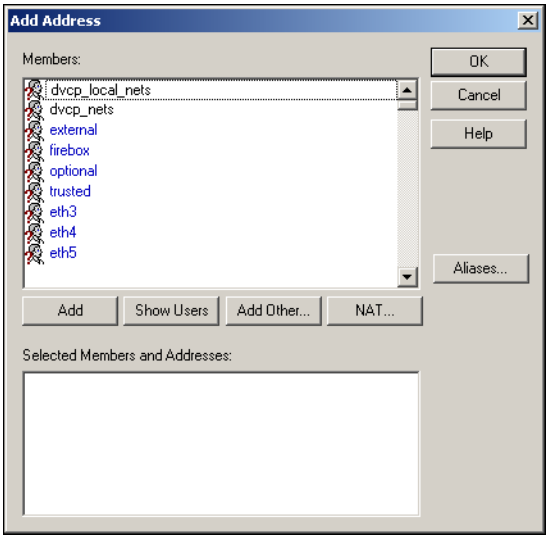


2 Click **Add**.
The Host Alias dialog box appears.

3 In the **Host Alias Name** text box, type the alias you use when you configure services and authentication.



4 Click **Add**.
The Add Address dialog box appears.



5 Add members to the alias. To add a member that appears in the **Members** list, click the name. Click **Add**.

6 To configure a new member, click **Add Other**.
The Add Member dialog box appears.

7 From the **Choose Type** drop-down list, select a category. In the **Value** text box, type the address, range, or host name. Click **OK**.

8 After you add the last member, click **OK**.
In the Host Alias dialog box the new alias appears. Click the alias to see its members.

To change an alias, select it, click **Edit**, and then add or erase the members.

To remove an alias, select it, click **Remove**. Then you have to remove the alias from the **Properties** box of all the services that use the alias.

For more information, refer to the “Defining Service Properties” on page 117.

How User Authentication Works

A special HTTP server operates on the Firebox®. To authenticate, a client must connect to the authentication server with a Web browser that can use Java. The address is:

http://*<IP address of a Firebox interface>*:4100/

A Java tool opens and the user must type a user name and password. The tool sends the name and password to the authentication server with a challenge and response protocol. When the server authenticates the user, the user must minimize the Java tool and the browser window. They can then use the approved network services. The user stays authenticated while the Java tool and the Firebox are active. To prevent an account from authenticating, you must disable the account on the authentication server.

Using external authentication

The primary function of the authentication tool is for outgoing traffic, but you can also use it for incoming network traffic. When you have an account on the Firebox, you can always do external authentication. For example, you can type this address in your browser at home:

http://<*public IP address of a Firebox interface*>:4100/

After authentication, you can get access to the services that are configured on the Firebox (FTP, Telnet).

Enabling remote authentication

Use this procedure to let a remote user authenticate from the external interface. This gives them access to services through the Firebox.

1. In the Services Arena in Policy Manager, select **View > Hidden Icons**. Double-click the wg_authentication service icon.
2. On the **Incoming** tab, select **Enabled and Allowed**.
3. Below the **From** box, click Add.
4. Click **Add Other**, and then type the IP addresses of the remote users that have approval to authenticate externally.

Authenticating from optional networks

1. In the Services Arena in Policy Manager, select **View > Hidden Icons**. Double-click the wg_authentication service icon.
2. On the **Incoming** tab, select **Enabled and Allowed**.
3. Below the **From** box, click **Add**.
4. Click **Add Other**, and then type the IP address, user, or group that can authenticate from an optional network.

Using authentication through a gateway Firebox to another Firebox

To send an authentication request through a gateway Firebox to a different Firebox you must add a policy allowing the authentication traffic on the gateway Firebox. On the gateway Firebox, add the wg_authentication service and allow traffic to the IP addresses of the destination Firebox.

Authentication Server Types

WatchGuard® System Manager can authenticate users for five different authentication server types:

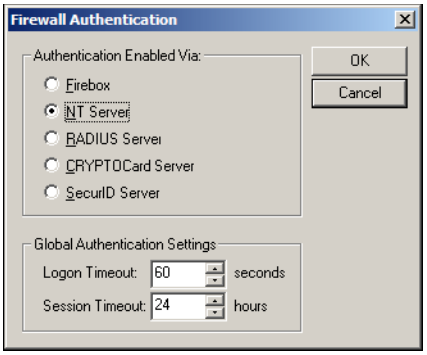
- The authentication server on the Firebox®
- NT primary domain controllers
- RADIUS-compliant authentication servers
- CRYPTOCard authentication servers
- SecurID authentication servers.

Authentication to the different servers is almost the same for the user. For the Firebox administrator, the difference is that the user database can be on the Firebox or on a different server.

When you use a different server, you must configure it with the instructions that its manufacturer gives. You must install the server with access to the Firebox and behind the Firebox for security.

To set the authentication type:

1 From Policy Manager, click **Setup** > **Firewall Authentication**.
Firewall Authentication Enabled Via dialog box appears.



2 In the **Authentication Enabled Via** dialog box, click an authentication server.

3 In the **Logon Timeout** text box, set the time interval (in seconds) that a user has to log in before the time-out stops the connection.

4 In the **Session Timeout** text box, set the time interval (in hours) that a connection can stay open, before the time-out stops the connection. This time does not change with the quantity of traffic.

Defining Firebox Users and Groups

If you do not use a third-party authentication server, you can use the Firebox® as an authentication server. You can divide your company into groups and users for authentication. Assign the members to groups because of the tasks, functions, or access requirements. For example, you can have an accounting group, a marketing group, and a research and development group. You can also have a new persons group, with a limit on Internet access.

In a group, you can set the authentication procedure for the users, their system type, and the information they have access to. A user can be a network or a computer. If your company changes, you can add or remove users or systems from groups.

Note

You can only have a specified number of Firebox users. With more than 100 users, WatchGuard recommends that you use a third-party authentication server.

WatchGuard® automatically adds two groups to the basic configuration for use in configuring a service for remote users:

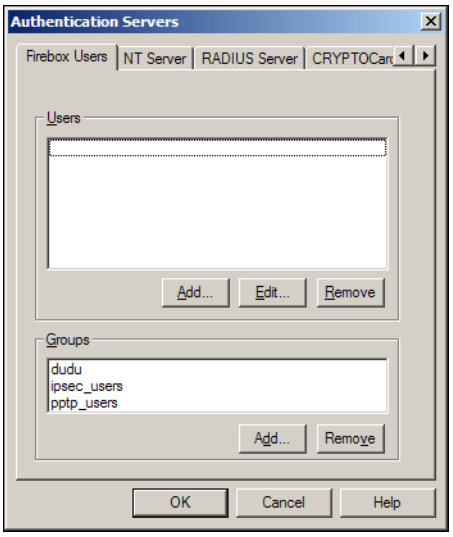
ipsec_users
Adds the names of approved users of MUVPN.

pptp_users
Adds the names of approved users of RUVPN with PPTP.

You can use Policy Manager to:

- Add, change or erase the groups in the configuration.
- Add or change the users in a group.

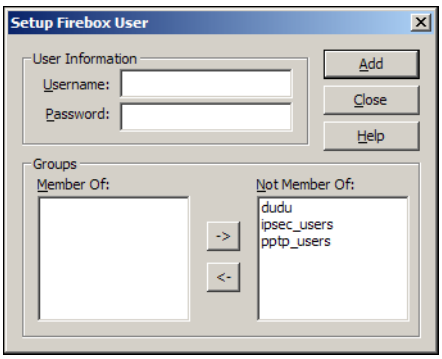
1 From Policy Manager, click **Setup** > **Authentication Servers**.
The Authentication Servers dialog box appears.



2 To add a new group, click the **Add** button below the **Groups** list.

3 Type the name of the group. Click **OK**.

4 To add a new user, click the **Add** button below the **Users** list.
The Setup Firebox User dialog box appears.



5 Type the user name and the password.

6 To add the user to a group, select the group name in the **Not Member Of** list. Click the arrow that points to the left side to move the name to the **Member Of** list.

7 After you add the user to all the groups, click **Add**.
The user adds to the User list. At this time you can add a different user.

8 To close the **Setup Firebox User** dialog box, click **Close**.
The Firebox Users tab appears with a list of the new users.

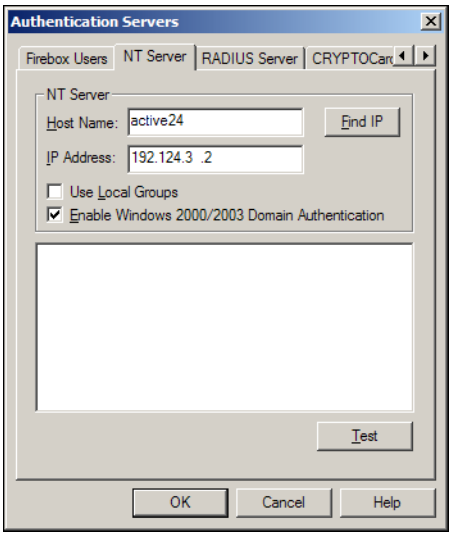
9 After you add all the users and the groups, click **OK**.
At this time, you can use the users and groups to configure services and authentication.

Configuring Windows NT Server Authentication

You can configure your Firebox to use the users and groups you make with a Windows NT server. Use the Policy Manager for WFS.

1 From Policy Manager, click **Setup** > **Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **NT Server** tab.



3 To identify the host, type the host name and the IP address of the Windows NT domain controller. If you do not know the IP address of the host, click **Find IP**. The IP address appears automatically.
When you type the IP addresses, type the digits and periods in the correct sequence. Do not use the TAB or arrow key to go by the periods.

4 If you want, select the **Use Local Groups** checkbox.
Windows NT has two group types: global and local. A local group is local to the security system in which it is created. A global group contains the user accounts from one domain put together as one group name. A global group cannot contain a different global group or a local group.

5 You can select the check box to enable access to the Windows Active Directory.

6 To try the authentication connection before you save the configuration, click **Test**. If you do not have the correct Windows Active Directory credentials, the **Active Directory Login** dialog box appears. Type the correct **Connect As** and **Password** information.
The Firebox connects to the NT server and shows the results.

7 Click **OK**.

Configuring RADIUS Server Authentication

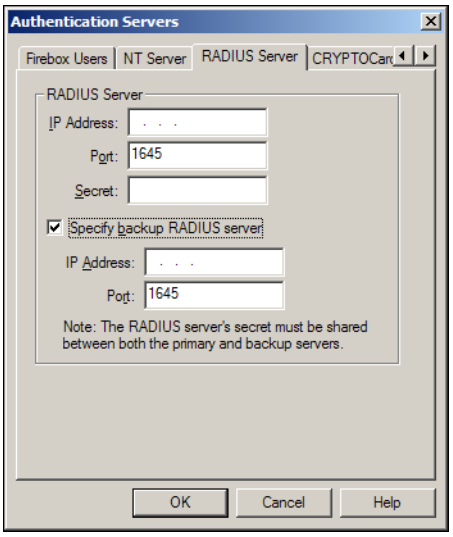
Remote Authentication Dial-In User Service (RADIUS) authenticates the remote users on a company network. RADIUS is a client and server system that keeps the authentication information for users, remote access servers, and VPN gateways in one database. This database is available to all users. RADIUS authenticates the full network from one location.

The authentication messages to and from the RADIUS server always have an authentication key. Note that the server sends the key, and not a password, during authentication. The client and the server each have the same key, or “shared secret”.

To add or remove a service for a user, you must change the RADIUS user (or group) in the service configuration on the Firebox®. You must also add the IP address of the Firebox to the RADIUS server. You can use CHAP or PAP authentication, but CHAP gives better security.

1 From Policy Manager, click **Setup** > **Authentication Servers**.

2 Click the **RADIUS Server** tab.
The RADIUS information appears.



3 In the **IP Address** text box, type the IP address of the RADIUS server.

4 Make sure that the port number RADIUS uses for authentication shows.
The default port number is 1645. RFC 2138 gives port number 1812, but many RADIUS servers use port number 1645.

5 In the **Secret** text box, type the "shared secret" between the Firebox and the RADIUS server.
The shared secret is case-sensitive and must be the same on the Firebox and the RADIUS server.

6 Type the IP address and the port of the backup RADIUS server. The shared secret must be on the primary and backup RADIUS server.

7 Click **OK**.

8 Get the IP address of the Firebox and the user or group aliases to authenticate with RADIUS. The aliases appear in the **From** and **To** boxes for each service.

To configure the RADIUS server

1 Add the IP address of the Firebox in the applicable fields. Refer to the RADIUS server instructions.
This is not necessary on all RADIUS servers.

2 Add the user groups used in your Policy Manager configuration to the Filter-IDs in the RADIUS configuration.
For more information, refer to the RADIUS server information.
For example, to add the groups Sales, Marketing, and Engineering type:
Filter-Id="Sales"
Filter-Id="Marketing"
Filter-Id="Engineering".

Note

The filter rules for the RADIUS user filter-IDs are case-sensitive.

Configuring CRYPTOCard Server Authentication

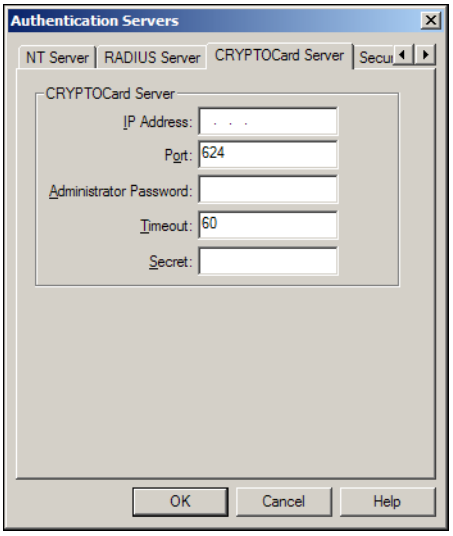
CRYPTOCard is a hardware-based authentication system that lets users authenticate with the CRYPTO-Card challenge and response system. This system includes off-line hashing of passwords. It enables you to authenticate a user independently of the computer they use.

When you configure WatchGuard CRYPTOCard authentication, you must first install a CRYPTOCard server. You must also have access to the server for authentication to the Firebox®.

To add or remove a service for a user, you must change the CRYPTOCard user (or group) in the service configuration on the Firebox. You must also add the IP address of the Firebox to CRYPTOCard authentication server.

1 From Policy Manager, click **Setup** > **Authentication Servers**.

2 Click the **CRYPTOCard Server** tab.
You can use the arrow keys in the top right corner of the dialog box to move this tab into view.



3 In the IP Address text box, type the IP address of CRYPTOCard server.

4 Make sure that the port number shows that CRYPTOCard authentication uses.
The standard port number is 624.

5 In the **Administrator Password** text box, type the administrator password that is in the password file on CRYPTOCard server.

6 Type or accept the time-out (in seconds).
The time-out is the maximum time that a user has to authenticate on CRYPTOCard server. CRYPTOCard recommends a maximum of 60 seconds.

7 In the **Secret** text box, type the shared secret between the Firebox and CRYPTOCard server.
This is the key or the client key in the "Peers" file on the CRYPTOCard server. This key is case sensitive and must be the same on the Firebox and CRYPTOCard server.

8 Click **OK**.

9 Get the IP address of the Firebox and the user or group aliases that CRYPTOCard must authenticate. The aliases appear in the **From** and **To** boxes for each service.

On the CRYPTOCard server:

1 Add the IP address of the Firebox in the applicable fields. Refer to the CRYPTOCard instructions.

2 Get the user or the group alias from the service properties. Add the aliases to the group information in the CRYPTOCard configuration file. You can only use one group with each user.
For more information, refer to the CRYPTOCard information.

Configuring SecurID Authentication

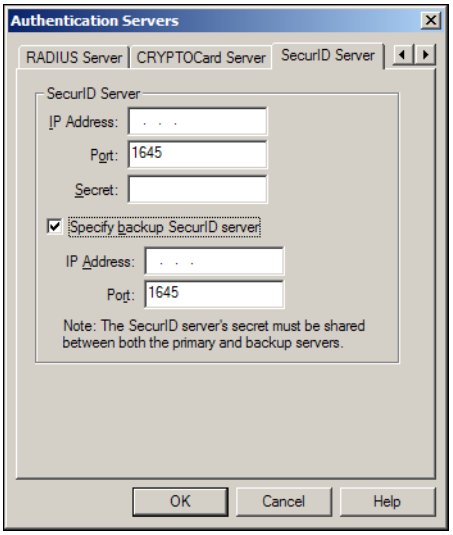
To operate SecurID authentication, you must configure RADIUS and ACE/Server servers correctly. The users must also have an approved SecurID token and a PIN. Refer to the SecurID instructions for more information.

Note

Do not use Steel Belted RADIUS with SecurID. Use RADIUS with RSA SecurID software.

1 From Policy Manager, click **Setup** > **Authentication Servers**.

2 Click the **SecurID Server** tab.
You can use the arrow keys in the top right corner of the dialog box to move this tab into view.



3 In the **IP Address** text box, type the IP address of the SecurID server.

4 Type or accept the port number for SecurID authentication.
The default number is 1645.

5 In the **Secret** text box, type the shared secret between the Firebox and SecurID server.
The shared secret is case-sensitive and must be the same on the Firebox and SecurID server.

6 If you use a backup server, select the **Specify backup SecurID server** check box. Type the IP address and the port number for the backup server.

7 Click **OK**.

To set up the RADIUS server, see "To configure the RADIUS server" on page 100

Configuring a Policy with User Authentication

After you have configured the Firebox® to use an authentication server, you can start to use user names when creating policies in Policy Manager. One method you can use is to put a limit on all policies that connections are allowed only for authenticated users. This is useful when you use DHCP on your network.

1 Create a group on your third-party authentication server that contains all the user accounts.

2 In Policy Manager, add or open your Outgoing service icon. On the Outgoing tab, allow outgoing traffic.

3 In the **From** field, type the group name you created on the authentication server.

4 Configure the other services in Policy Manager the same way.

5 After you add a user or group to a policy configuration, use the WG-Auth policy that appears in Policy Manager to control access to the authentication Web page.

CHAPTER 10

Intrusion Detection and Prevention

The WatchGuard® System Manager protects your network from many attack types when it applies the packet filters and proxies that you set up. For the attacks that these filters and proxies cannot prevent, the Firebox® has these tools:

Default packet handling
: Helps identify the incoming traffic that appears to be an attack on a network.

Blocked sites
: Helps to prevent incoming traffic from computer systems you know or think are a security risk. This tool denies an external IP address, and it cannot connect to an internal host.

Blocked ports
: Helps deny use of external ports that can be attacked by a hacker. A blocked port stops all the packets that try to use a specified port, thus no incoming traffic can use that port to enter your network.

Your log configuration can help you to identify the Web sites that show suspicious activity (spoofing). You can then manually and permanently deny these Web sites or the ports they use. For more information on the log messages, refer to the FAQ:

www.watchguard.com/support/advancedfaqs/log_main.asp

Default Packet Handling

The Firebox® examines the source and destination of each packet it receives. It looks at the IP address and the port number. It also monitors the packets to look for patterns that can show that your network is at risk. With default packet handling options, you can set the Firebox to:

- Reject a packet that can be a security risk
- Automatically deny all traffic from a source IP address
- Add an event to the log file
- Send a notification of a possible security risk

Blocking spoofing attacks

One method that a hacker can use to get access to your network is to create an electronic "false identity." With this "IP spoofing" procedure, the attacker makes a TCP/IP packet that uses a different IP address than the host it comes from.

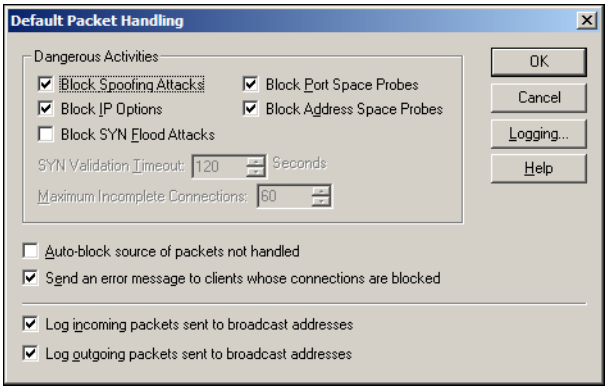
A router uses the destination address of a packet to forward it to its destination. Thus, the source address of the packet is not authenticated until the packet gets to its destination. If a host is a "trusted host", authentication is not necessary. In IP spoofing, an attacker can use this information to route a packet as if it comes from a trusted host. The destination system then authenticates the IP address of the connection and gives access through your firewall.

You can enable protection for IP spoofing on the Firebox. The Firebox denies the spoofed packets, and then sends two log messages. One log message shows that the packet of the attacker was blocked. The Firebox sends a second log message to show that the attacker IP address is on the Blocked Sites list. All the Web sites that the Firebox denies appear on the Blocked Sites list.

1 From Policy Manager, select **Setup > Intrusion Prevention > Default Packet Handling**.

Or,
click the Default Packet Handling icon on the Policy Manager toolbar.

2 Select the **Block Spoofing Attacks** check box.



Blocking port space and address space attacks

An attacker can also use probes to get access to your network. A *port space probe* examines a host to find the filters and proxies that it uses. An *address space probe* examines a network to see the services that operate on the hosts in that network.

1 From Policy Manager, select **Setup > Intrusion Prevention > Default Packet Handling**.

Or,
click the Default Packet Handling icon on the Policy Manager toolbar

2 Select the **Block Port Space Probes** check box.

3 Select the **Block Address Space Probes** check box.

Stopping IP options attacks

IP options are extensions of the Internet Protocol. The Firebox uses the extensions for special software applications or for advanced troubleshooting. An attacker can use the I**P options** in the packet header to find a path into your network.

1 From Policy Manager, select **Setup** > **Intrusion Prevention** > **Default Packet Handling**.

Or,
click the Default Packet Handling icon on the Policy Manager toolbar.

2Select the **Block IP Options** check box.

Stopping SYN Flood attacks

A SYN Flood attack is a type of Denial of Service (DoS) attack. This attack tries to prevent access to your public services (e.g. e-mail, Web servers) by unauthorized users. The SYN Flood attack uses a part of the usual TCP connection procedure to attack. The usual TCP procedure is as follows:

- A user tries to connect to your server using their Web browser. To do this, the browser sends a SYN segment.
- Your Web server sends a SYN+ACK segment.
- The browser then sends an ACK segment.
- When the server sees the ACK segment, it can accept the URL from the browser.

Until the server receives the ACK segment, the server is "stuck". Many servers can accept only a specified number of open connections at a time. The server keeps them in a backlog until they are completed or time-out. A SYN Flood attack tries to fill up the backlog of the server. It sends many SYN segments and no ACK. When the backlog is full, the server is not available to the users.

The WatchGuard® System Manager can help protect your servers against a SYN Flood attack. It monitors the number of SYN segments without an ACK segment. If this number gets larger than the specified maximum, the SYN Flood protection starts and all new connections must have verification. The SYN Flood protection tool stops when the attack stops.

1 From Policy Manager, select **Setup** > **Intrusion Prevention** > **Default Packet Handling**.

Or,
click the Default Packet Handling icon on the Policy Manager toolbar.

2 Select the **Block SYN Flood Attacks** check box.

Changing SYN flood settings

When the Firebox® blocks SYN Floods, it can also keep regular packets from your network. You can change the SYN Flood configuration to help prevent this. You can set the number of **Maximum Incomplete Connections** that the Firebox lets through before the Firebox starts to block connections. The default number is 60. When there are 61 connections that do not receive an ACK, the Firebox blocks all additional connections. It stops when the number decreases to 59.

To see how frequently the feature starts, you can look in the log for:

```
SYN Validation: activated and SYN Validation: deactivated
```

When there are many of these messages and no attacks, the number of Maximum Incomplete Connections could be set too low. When the attacks are not being stopped, the number could be too high.

The **SYN validation timeout** controls how long the Firebox "remembers" clients that have validation. The default time-out is 120 seconds, so a client can connect again in that 120 seconds with no validation. With a time-out of zero, each connection must have validation.

1 From Policy Manager, select **Setup** > **Intrusion Prevention** > **Default Packet Handling**.

Or,
click the Default Packet Handling icon on the Policy Manager toolbar.

2 Set the **SYN Validation Timeout** value.

3 Set the **Maximum Incomplete Connections** value.

Unhandled packets

An "unhandled" packet is a packet that does not match any rule created in Policy Manager. The Firebox always denies the packet, but you can select to always automatically block the source. This adds the IP address that sent the packet to the temporary blocked sites list. You can also send a TCP reset or ICMP error back to the client when an unhandled packet is received by the Firebox.

Blocking Sites

The Blocked Sites feature helps to prevent communication between your users and systems you know or think are dangerous or a security risk. After you identify the site, you can block all the connections with that IP address. You can also configure logging to record all access from this source. From the log file, you can find the services that they use to attack.

A blocked site is an external IP address that can not make a connection to an internal host. If a packet comes from a system that is blocked, it does not get through the Firebox®.

There are two types of blocked sites:

- Permanently blocked sites — on a list in the configuration file that you can change only manually.
- Auto-blocked sites — The sites that the Firebox adds or removes on a temporary blocked site list. The Firebox uses the packet handling rules which are specified for each service.
  For example, you can configure the Firebox to block the sites that try to connect to a blocked port. These sites are then blocked for a specified time.

  For information on the automatic blocking of sites with the protocol anomaly detection (PAD) tool, refer to the "Configuring Incoming SMTP Proxy" on page 71.

Auto-blocking and logging can help you make a decision about which sites to block. For example, you can add a site that does IP spoofing to the list of the permanently blocked sites.

Note

You can block only external IP addresses.

Blocking a site permanently

You can use the Policy Manager for WFS to permanently block a host that you know is a security risk. For example, a university computer that hackers use frequently is a good host to block. The default configuration blocks 3 private ("unconnected") network addresses—10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Packets from these private addresses can not go through the Firebox. Packets that come from one of

these addresses could be using IP spoofing. For more information on these addresses, refer to RFCs 1918, 1627, and 1597.

1 From Policy Manager, select **Setup** > **Intrusion Prevention** > **Blocked Sites**.

Or,
click the Block Sites icon on the Policy Manager toolbar.

2 Click **Add**.

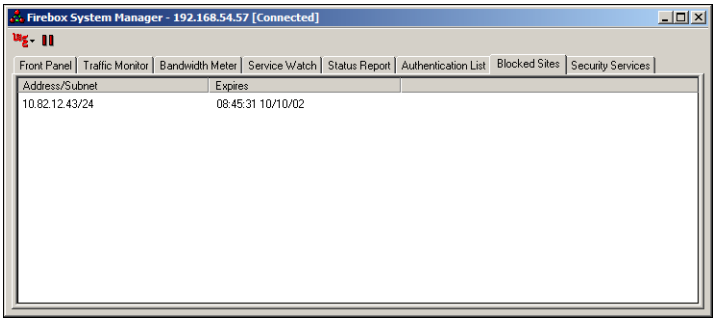
3 From the **Choose Type** drop-down list, select **Host IP Address, Network IP Address,** or **Host Range**.

4 Type the member value.

The member type shows if this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the stop. Do not use the TAB or the arrow key.

5 Click **OK**.

If you connect to the Firebox using Firebox System Manager, the new site appears in the Firebox System Manager Blocked Sites list.



Using an external list of blocked sites

You can make a list of blocked sites in an external file. This file must be a `.txt` file. To add an external file to your blocked sites list:

1 In the **Blocked Sites**, select **Import**.

2 Find the file. Double-click it, or select it and select **Open**.

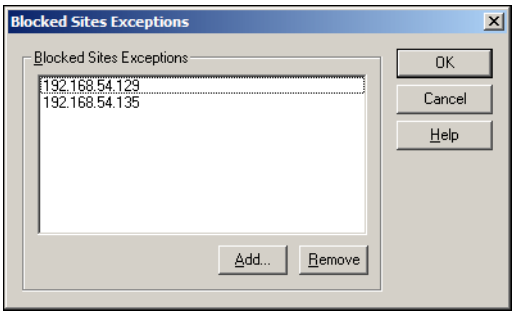
The sites in the file add to the Blocked Sites list.

Creating exceptions to the Blocked Sites list

The Firebox does not add to the list of automatically blocked sites a host that is on its exception list even if it sends suspect traffic. The automatic rules do not apply for this host.

1 From Policy Manager, click **Setup** > **Intrusion Prevention** > **Blocked Sites Exceptions**.

The Blocked Sites Exceptions dialog box appears.



2 Click **Add**.

3 Type the IP address of the site. Select **OK**.

4 Click **OK**.

To remove an exception, select the IP address of the site to remove. Click **Remove**.

Changing the auto-block duration

From **Blocked Sites,** you can change the interval, in minutes, that the firewall automatically blocks an IP address that is a security risk. The interval can be from 1 to 32,000 minutes (about 22 days).

Logging and notification for blocked sites

The Firebox can send a log message for each sites that it blocks.

1 From Policy Manager, click **Setup** > **Intrusion Prevention. Blocked Sites**. Click **Logging**.

2 In the **Category** list, select **Blocked Sites**.

3 Change the logging and the notification configuration.

Blocking Ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. If you block a port, you override all the service configurations.

Note

The Blocked Ports, as do the Blocked Sites, only block the packets that come through the external interface.

You can block a port, because:

- Blocked Ports protect your most sensitive services. The feature helps protect you from errors in your Firebox configuration.
- Probes against very sensitive services can make independent log entries.
- Some TCP/IP services use port numbers of more than 1024. An attack on these ports is possible if the attacker uses an approved service, with a port number of less than 1024. The attacker then makes it appear as an approved connection in the opposite direction. You can prevent this, if you block the port numbers of services with port numbers of less than 1024.

By default, the Firebox blocks some destination ports. This gives a basic configuration which you usually do not have to change. Default blocked ports are blocked for TCP and UDP, and include::

X Window System (ports 6000-6005)

The X Window System (or X-Windows) client connection is not encrypted and is dangerous to use on the Internet.

X Font Server (port 7100)

Many versions of X-Windows can operate X Font Servers. The X Font Servers operate as the super-user on some hosts.

NFS (port 2049)

NFS (Network File System) is a much used TCP/IP service, where many users can use the same files on a network. But, the new versions have important authentication and security problems. To supply NFS service through the Internet can be very dangerous.

Note

The portmapper frequently uses the port 2049 for NFS. If you use NFS, make sure that NFS uses the port 2049 on all your systems.

rlogin, rsh, rcp (ports 513, 514)

These services give remote access to other computers. They are a security risk and many attackers probe for these services.

RPC portmapper (port 111)

The RPC Services use port 111 to find which ports a given RPC server uses. The RPC services are very easy to attack through the Internet.

port 0

IANA can use Port 0. Many software applications that examine ports start on port 0.

port 1

The TCPmux service uses Port 1, but not very frequently. You can block it to make it more difficult for the tools that examine ports.

port 8000

This port is used by multiple vendors and has multiple security problems recorded against it.

Avoiding problems with approved users

Approved users can have a problem because of blocked ports. You must be very careful if you block the port numbers between 1000 through 1999. Client ports frequently use these numbers.

Note

Solaris uses port numbers higher than 32768 for clients.

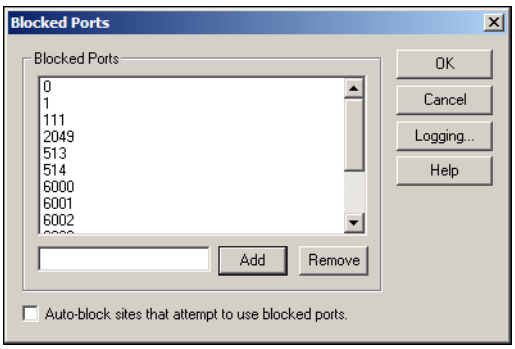
Blocking a port permanently

You can set the Firebox to block ports so that no external host can connect with that port. The default configuration automatically blocks ports that security experts consider dangerous.

1 From Policy Manager, select **Setup** > **Intrusion Prevention** > **Blocked Ports**.

Or,
click the Blocked Ports icon on the Policy Manager toolbar.

2 In the box on the left side of the **Add** button, type the port number. Click **Add**.
The new port number appears in the Blocked Ports list.



To remove a blocked port, select the port to remove. Click **Remove**.

Auto-blocking sites that try to use blocked ports

You can configure the Firebox to automatically block an external host that tries to get access to a blocked port. In the Blocked Ports dialog box, select the **Auto–block sites that attempt to use blocked ports** check box.

You can also block sites automatically if you use protocol anomaly detection. For more information, refer to the "Configuring Incoming SMTP Proxy" on page 71.

Logging and notification for blocked ports

The Firebox can send a log message for each port that it blocks.

1 From Policy Manager, click **Setup** > **Intrusion Prevention. Blocked Ports**. Click **Logging**.

2 In the **Category** list, select **Blocked Ports**.

3 Change the logging and the notification configuration.
For more information, see the WatchGuard System Manager User Guide chapters on the log server and log configuration.

Blocking Sites Temporarily with Service Settings

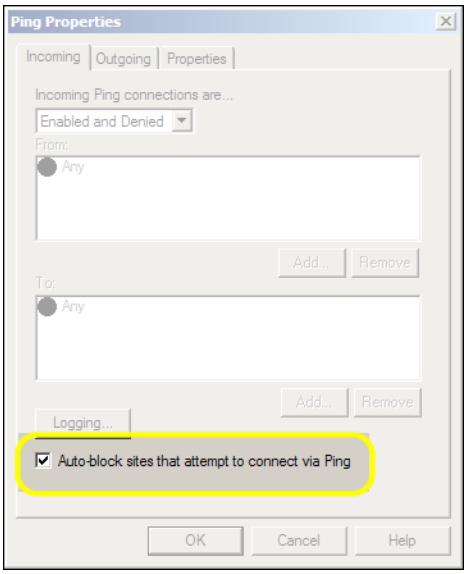
You can use the service configuration to automatically and temporarily block sites that try to use a denied service. You can use this feature to log, block, and monitor each site that tries to get access to a blocked port.

Configuring a service to temporarily block sites

1 From Policy Manager, double-click the service icon in the Services Arena.
The Properties dialog box appears.

2 From the **Incoming service Connections Are** drop-down list, select **Enabled and Denied**.

3 Select the **Auto-block sites that attempt to connect via service** check box.



Viewing the Blocked Sites list

The Blocked Sites list shows all the sites that the Firebox® blocks. Use the Firebox System Manager to see the sites that are automatically blocked by the property configuration of a service. From the Firebox System Manager, select the **Blocked Site List** tab.

Integrating Intrusion Detection

A good intrusion detection system (IDS) examines the traffic that tries to get access to your network. It looks at the source, the destination, and the type of traffic for a period of time. The IDS then compares the traffic against the attack configurations that are known. When the IDS finds an attack, it can tell you the type of the attack and the possible steps to do.

The primary function of your firewall is to examine and allow or deny packets. It is a basic IDS, and it stops some basic attacks including IP spoofing and port space probes. There is not much bandwidth available in the Firebox® for it to look at patterns of traffic through time.

As part of your LiveSecurity® Service subscription, you can download the Firebox System Intrusion Detection System Mate (fbidsmate) tool. With this tool, the Firebox can communicate with most commercial and shareware IDS applications. You use the fbidsmate tool to configure your IDS to use programs that get data from the Firebox. Versions are available for the Win32 (Windows NT, Windows 2000, and Windows XP), the SunOS, and the Linux operating systems. The fbidsmate-tool can also add log messages to the log file, that you can then use in reports. And because the fbidsmate tool is external to the Firebox, you do not have to change the Firebox configuration.

An external IDS software application can automatically add sites to the Blocked Sites list of the Firebox. These sites appear in the **Blocked Sites** tab of the Firebox. The time-outs and the blocked site exceptions features are the same as for sites blocked by the **default packet handling options**.

You can get the fbidsmate tool with your LiveSecurity Service account at:

www.watchguard.com/support

Using the fbidsmate tool

The fbidsmate tool operates from the command line. You can use an IDS software application or use the commands directly against the Firebox. You give the command as follows:

```
fbidsmate firebox_address [rwpassphrase | -f rwpassphrase_file] [add_hostile hostile_address] | [add_log_message priority(0-7) "message"]
fbidsmate import_passphrase rwpassphrase rwpassphrase_filename
```

add_hostile

This adds an IP address to the Auto-Blocked Site list for the time interval set by the administrator in the dialog box for the **Blocked Sites** in the Policy Manager.

add_log_message

This adds a log message in the log that the Firebox makes. The Firebox uses the priority to make syslog messages. The range is the standard syslog 0=Emergency to 7=Debug. There is no limit on the message length. If necessary, the Firebox divides the text in more than one message.

import_passphrase

You can keep the Firebox configuration passphrase in an encrypted file, as an alternative to clear text in the program command. This command puts the passphrase in the specified file with 3DES encryption. At this time, you can use the file name in your software application. Each Firebox has a special passphrase.

Return value

The return value of fbidsmate is zero if the software application operated correctly; if not it is not zero. You must examine this value if you operate fbidsmate from a third-party software application or through a different interface.

Examples

Here are some examples, where the IP address of the Firebox is 10.0.0.1, and the configuration passphrase is "secure1".

Example 1

The IDS senses a port scan from 209.54.94.99 and tells the Firebox to block that site:

```
fbidsmate 10.0.0.1 secure1 add_hostile 209.54.94.99
```

This message appears in the log file:

```
Temporarily blocking host 209.54.94.99
```

Example 2

The IDS adds a message to the log of the Firebox:

```
fbidsmate 10.0.0.1 secure1 add_log_message 3 "IDS system temp. blocked 209.54.94.99"
```

If the IDS operates on host 10.0.0.2, this message appears in the Firebox log file:

```
msg from 10.0.0.2: IDS system temp. blocked 209.54.94.99
```

Example 3

You operate an external IDS application. You can encrypt the configuration passphrase that you use in your IDS program.

Note

You must also give the best possible security to the IDS host.

First, you must move the passphrase "secure1" to an encrypted file on the IDS host:

```
fbidsmate import_passphrase secure1 /etc/fbidsmate.passphrase
```

Then you can rewrite the examples 1 and 2, as:

```
fbidsmate 10.0.0.1 -f /etc/fbidsmate.passphrase add_hostile 209.54.94.99
fbidsmate 10.0.0.1 -f /etc/fbidsmate.passphrase add_log_message 3 "IDS system temp. blocked 209.54.94.99"
```

CHAPTER 11

Connecting with Out-of-Band Management

With the Out-Of-Band (OOB) management feature of the WFS appliance software, you can connect to the Firebox® with a modem and a telephone line. You must purchase the modem separately. With OOB you can change the configuration of the Firebox from a remote location without the use of the Firebox Ethernet interfaces. Support for OOB is not included with Fireware Pro appliance software.

Connecting a Firebox with OOB Management

To use the OOB feature to connect to the Firebox®, you must:

- Connect a modem to the serial port of the Management Station.
- Connect a telephone line to the modem.
- Connect an external modem or a PCMCIA/PC Card modem to the Firebox. If you use an external modem, you must attach it to the Console port of the Firebox.
- Enable the Management Station for dial-up networking.
- Set the Firebox network configuration.

Enabling the Management Station

You must configure the Management Station to use a PPP connection. The Windows NT, Windows 2000, and Windows XP platforms each have a different procedure.

Preparing a Windows NT management station for OOB

Install the Microsoft Remote-Access-Server (RAS) on the management station:

1. Attach a modem to your computer with the instructions from the manufacturer.
2. From the Windows NT Desktop, click **Start** > **Settings** > **Control Panel**.
3. Double-click **Network.**

4 Click **Add.**
The Select Network Service dialog box appears.
5 Click **Remote Access Server**. Click **OK**.
Follow the steps to complete the installation. If necessary, you must install Dial-Up Networking.

Preparing a Windows 2000 management station for OOB

Make sure that the modem is installed. If necessary, follow the procedure below. Then you can configure the dial-up connection.

Install the modem

1 From the Desktop, click **Start** > **Settings** > **Control Panel** >**Phone and Modem Options**.
2 Click the **Modems** tab.
3 Click **Add**.
The Add/Remove Hardware Wizard appears.
4 Follow the steps of the wizard and complete the information requests.
Make sure you have the name and model of the Firebox modem and the modem speed.
5 Click **Finish** to complete the modem installation.

Configure the dial-up connection

1 From the Desktop, click **My Network Places** > **Network and Dial-up Connections** > **Make New Connection**.
The Network Connection wizard appears.
2 Click **Next**. Click **Dial up to Private Network**. Click **Next**.
3 The modem in the Firebox connects to a telephone line. Type the number of that telephone line. Click **Next**.
4 Choose the designation for your connection. Click **Next**.
5 Type a name for your connection.
This name shows with the icon. Type a name that gives the function of the icon, for example, OOB Connection.
6 Click **Finish**.
7 Click **Dial** or **Cancel**.

The new icon shows in the Network and Dial-Up Connections. To use this dial-up connection, double-click the icon.

Preparing a Windows XP management station for OOB

Make sure that the modem is installed. If necessary, follow the procedure below. Then you can configure the dial-up connection.

Install the modem

1 Click **Start** > **Control Panel** > **Phone and Modem Options**.
2 Click the **Modems** tab.
3 Click **Add**.
The Add Hardware Wizard shows.
4 Follow the steps of the wizard.
NOTE: You have to know the name and model of the Firebox modem and the modem speed.

5 Click **Finish** to complete the modem installation.

Configure the dial-up connection

1 Click **Start** > **Control Panel** > **Network Connections**. Click **New Connection Wizard**.
The New Connection Wizard appears.

2 Click **Next**. Click **Connect to the network at my workplace**. Click **Next**.

3 Click **Dialup connection**. Click **Next**.

4 Type a name for your connection.
This name shows with the icon. Type a name that gives the function of the icon, for example, OOB Connection.

5 The modem in the Firebox connects to a telephone line. Type the number of that telephone line. Click **Next**.

6 Click **Finish**.

7 Click **Dial** or **Cancel**.

The new icon shows in the Network Connections. To use this dial-up connection, double-click the icon.

Configuring the Firebox for OOB

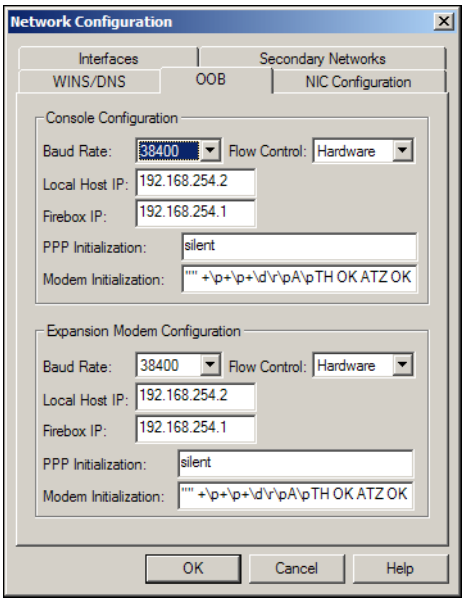
You can configure the OOB management features in the Policy Manager. In the Network Configuration dialog box, click the OOB tab:

- In the top of the dialog box, you can control the properties of an attached external modem.
- In the bottom of the dialog box, you can configure an installed PCMCIA modem.

The OOB management features are automatically enabled on the Firebox during initial configuration.

The first time you connect to a Firebox® with OOB, the Firebox uses the default OOB properties.

1 From Policy Manager, click **Network** > **Configuration**. Click the **OOB** tab.



2 Change the OOB properties to match your security preferences. Click **OK**.
For a description of each control, right-click it, and then select What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

Establishing an OOB Connection

- From the Management Station, use dial-up networking to make a connection to the Firebox modem.
- The modems connect.
- The Firebox® makes a PPP connection with the Management Station to let IP traffic through.
- With the dial-up PPP address of the Firebox you can use the WatchGuard® System Manager. The default address is 192.168.254.1.

Configuring PPP to connect to a Firebox

In the default configuration, Firebox PPP accepts a connection from a standard computer. The configuration of your management station is almost the same as for a typical Internet service provider. It is not necessary to type a user name or password.

OOB time-out disconnects

The Firebox starts the PPP session. The Policy Manager on your management station makes a secure connection to the Firebox. If the Firebox has no secure connection in a default period of 90 seconds, the Firebox stops the session.

PART III Virtual Private Networking

CHAPTER 12

Configuring BOVPN with Manual IPSec

You use Branch Office VPN (BOVPN) with manual IPSec to make encrypted tunnels between a Firebox® and an IPSec-compliant security device. This device can protect a branch office, or another remote site. BOVPN with Manual IPSec is available for the WatchGuard® System Manager with medium encryption version at DES (56-bit). It is also available for the WatchGuard System Manager strong encryption versions at DES (56-bit) or 3DES (168-bit).

Note

The Firebox X500 does not use BOVPN unless you purchase the BOVPN Upgrade. Firebox X700, Firebox X1000, and Firebox X2500 use BOVPN only if you register the device with LiveSecurity Service. To upgrade the Firebox X500 to use BOVPN, see "Enabling the BOVPN Upgrade" on page 131.

Note

You cannot configure a Manual IPSec tunnel with a Firebox or device that is configured as a DHCP or PPPoE client. The two devices must have static public IP addresses. Also, Manual IPSec tunnels do not have support for incoming static NAT.

Configuration Checklist

You must have the following information to use BOVPN with Manual IPSec:

- Public IP addresses for the two ends of the tunnel
- Policy endpoints — IP addresses of special hosts or networks that operate on the tunnel
- Encryption method (the two ends of the tunnel must use the same encryption method)
- Authentication method

Configuring a Gateway

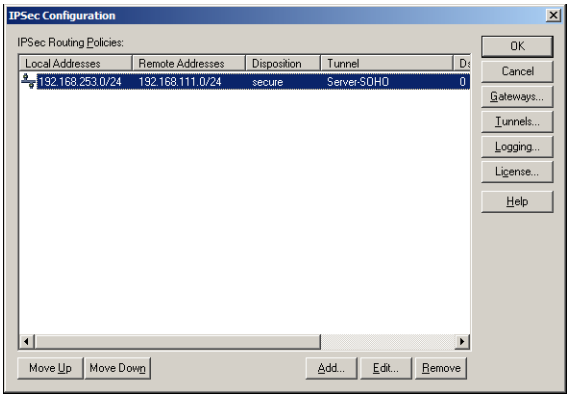
A gateway is a connection point for one or more tunnels. The gateway standard connection method becomes the standard connection method for tunnels made with the device at the other end of the tunnel. An example is ISAKMP automated key negotiation.

Adding a gateway

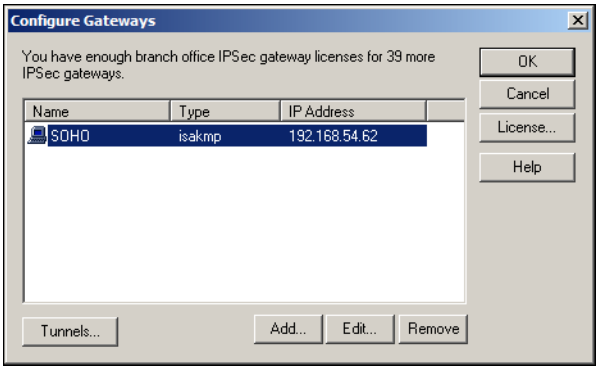
To start IPSec tunnel negotiation, one peer must connect to the other. To do this, you can use an IP address or a DNS name. If the peer is dynamic, you cannot use an IP address.

If the peer uses dynamic DNS, you can configure the Firebox® to use dynamic DNS. The Firebox can then change the DNS name into an IP address, and the negotiation can start. To configure this, set the ID type of the remote gateway to D**omain Name**. Set the name of the peer to the fully qualified domain name. Set the DNS server of the Firebox to one that can identify the name, usually an internal DNS server.

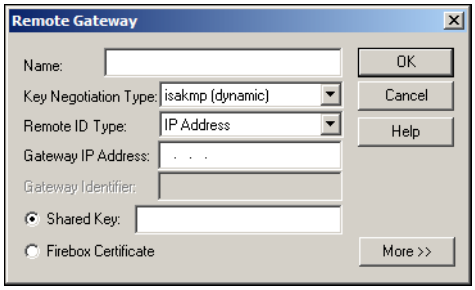
1 From Policy Manager, click **Network** > **Branch Office VPN** > **Manual IPSec**.
The IPSec Configuration dialog box appears. The Manual IPSec menu option is not enabled if you have a Firebox X500 and did not get the BOVPN Upgrade.



2 Click **Gateways**.
The Configure Gateways dialog box appears.



3 To add a gateway, click **Add**.
The Remote Gateway dialog box appears.



4 In the Name text box, type the gateway name.
This name identifies the gateway only in the Policy Manager.

5 From the **Key Negotiation Type** drop-down list, select **ISAKMP (dynamic)** or **Manual**.

6 From the **Remote ID Type** drop-down list, select IP Address, Domain Name, or User Name.
The Firebox uses IP Address and Domain Name to find the VPN endpoint. User name is a label that you use to identify the user at the VPN endpoint.

Note

WatchGuard recommends that you use the default value for the IP Address in the Remote ID Type text box. This is the external IP address of the Firebox. If you must change this value, examine the applicable interoperability document. This document has the information on the values you must use in this text box.

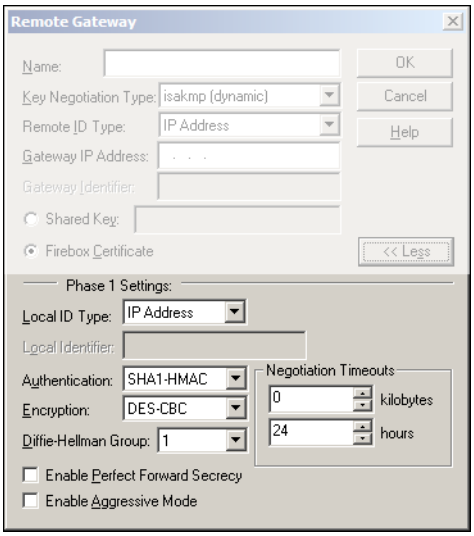
7 In the **Gateway IP Address** text box, type the IP address or identification of the gateway.
Use the domain name as the identification if the Firebox X Edge or SOHO uses DHCP or PPPoE for its external IP address. This information is in the Firebox configuration.

8 Click **Shared Key** or **Firebox Certificate** to identify the authentication procedure that you want to use. If you select **Shared Key**, type the shared key.
These selections are available only for ISAKMP-negotiated gateways. You must use the same key at the remote device.

Note

You must start the certificate authority on the Firebox if you select to authenticate with certificates. For information on this, see ***Chapter 19, “Activating the Certificate Authority on the Firebox.”*** In addition, if you use certificates, you must use the WatchGuard Security Event Processor for logging.

9 To configure Phase 1, click **More**.
The Phase 1 properties fields appear. Phase 1 applies to the initial phase of the IKE negotiation. It contains authentication, session negotiation, and key change information.



10 From the **Local ID Type** drop-down list, select **IP Address**, **Domain Name**, or **User Name**.
The Firebox uses IP Address and Domain Name to find the VPN endpoint. User name identifies the user at the VPN endpoint.

Note

For VPN tunnels with WatchGuard devices, WatchGuard recommends you use the default value in the Local ID Type field. This is the external IP address of the Firebox. If you must change this value, examine the applicable interoperability document. This document has the information on the values you must use in this field.

11 From the **Authentication** drop-down list, select the type of authentication: **SHA1-HMAC** or **MD5-HMAC**.

12 From the **Encryption drop-down list**, select the type of encryption: **DES-CBC** or **3DES-CBC**.

13 From the **Diffie-Hellman Group** drop-down list, select the group. WatchGuard supports groups 1 and 2.
Diffie-Hellman refers to a mathematical procedure to safely negotiate secret keys across a public medium. Diffie-Hellman groups are sets of properties that you use to get this. Group 2 is more safe than group 1, but takes more time to make the keys.

14 If you select Diffie-Hellman group 1, select the **Enable Perfect Forward Secrecy** check box
When you select this, each new key that is negotiated gets a new Diffie-Hellman interchange. This as an alternative to getting only one Diffie-Hellman interchange. Enabling this gives more security, but uses more time.

15 If you select Diffie-Hellman group 2, select the **Enable Aggressive Mode** check box
This mode refers to an interchange of messages in Phase 1. The Main Mode is the default mode.

16 Type the negotiation time-outs in kilobytes, hours, or kilobytes and hours.
If you select kilobytes and hours, the time-out occurs at the time that comes first. You can type the time-out values or use the value control to set the values.

17 When you complete the entries, click **OK** to get back to the **IPSec Configuration** dialog box.

Editing and removing a gateway

To change a gateway, from the Configure Gateways dialog box:

1 Select the gateway and click **Edit**.
The **Remote Gateway** dialog box appears.

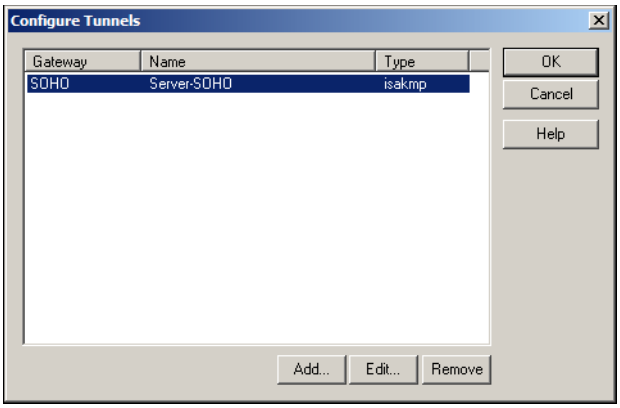
2 Make the changes and click **OK**.

To remove a gateway from the **Configure Gateways** dialog box, select the gateway and click **Remove**.

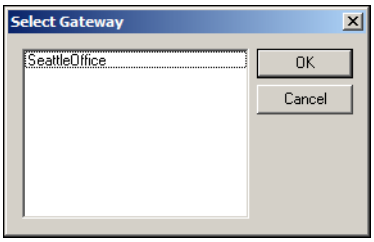
Making a Tunnel with Manual Security

You can configure a tunnel that uses a gateway with the manual key negotiation type.

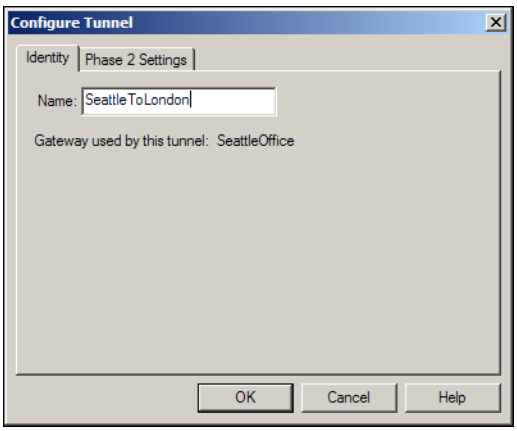
1 From Policy Manager, select **Network** > **Branch Office VPN** > **Manual IPSec**. Click **Tunnels**.
The Configure Tunnels dialog box appears.



2 Click **Add**.
The Select Gateway dialog box appears.



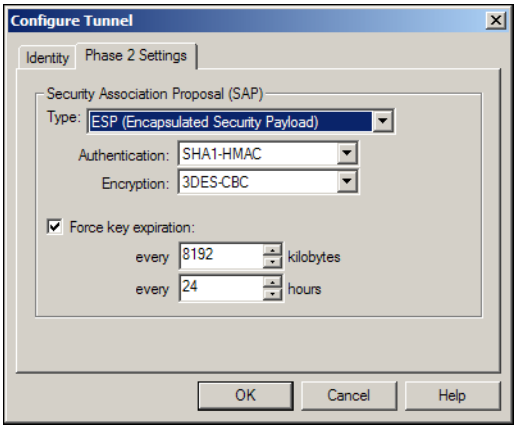
3 Select a remote gateway with manual key negotiation type to connect with this tunnel. The **Type** column at the dialog box of the **Configure Tunnels** shows the key negotiation type. Click **OK**.
The Identity tab of the dialog box of the Configure Tunnel appears.



4 Type a tunnel name.
Policy Manager uses the tunnel name as an identifier.

5 Click the **Manual Security** tab. Click **Settings**.
The Incoming tab of the **Security Association Setup** dialog box appears.

6 Click the **Phase 2 Settings** tab.



7 Click the ESP or AH security type. Configure the selected security type.
The difference between the two is that ESP is authentication with encryption, while AH is authentication only. Also, ESP authentication does not include the IP header, while AH does. The use of AH is rare.
For more information about configuring the security procedure, see "Using Encapsulated Security Protocol (ESP)" on page 126 and "Using Authenticated Headers (AH)" on page 127.

8 To use the same parameters for incoming traffic and outgoing traffic, select the **Use Incoming Settings for Outgoing** check box.

9 If you select this check box, you have completed the **Security Association Setup** dialog box. You can continue with the subsequent step. If you clear this check box, click the Outgoing tab and configure the security associations for outgoing traffic. The fields have the same rules and parameter ranges as the Incoming tab. When you finish, click **OK**.
The **Configure Gateways** dialog box appears, and shows the new tunnel. Do the make tunnel procedure again until you complete all tunnels for this gateway.

10 After you add all tunnels for this gateway, click **OK**.
The **Configure Gateways** dialog box appears. To configure more tunnels for a second gateway, click **Tunnels**. Select a new gateway and do the tunnel procedure again for that gateway.

11 When all the tunnels are complete, click **OK**.

Using Encapsulated Security Protocol (ESP)

1 Type or use the SPI spin control to identify the Security Parameter Index (SPI).
You must select a number between 257 and 1023.

2 From the **Encryption** drop-down list, select an encryption algorithm.
Select from: None (no encryption), DES-CBC (56-bit), and 3DES-CBC (168-bit).

3 If you selected **DES-CBC** or **3DES-CBC**, click **Key**.

4 Type a passphrase to supply a key. Click **OK**.
The passphrase appears in the Encryption Key field. You cannot type a key in that field directly.

5 From the **Authentication** drop-down list, select an authentication algorithm.
Select from: None (no authentication), MD5-HMAC (128-bit algorithm), or SHA1-HMAC (160-bit algorithm).

6 If you selected **MD5-HMAC** or **SHA1-HMAC**, click **Key**.

7 Type a passphrase to supply a key. Click **OK**.
The passphrase appears in the Authentication Key field. You cannot type a key here directly.

Using Authenticated Headers (AH)

1 Type or use the SPI spin control to identify the Security Parameter Index (SPI).
You must select a number between 257 and 1023.

2 Use the **Authentication** drop-down list to select an authentication method.
Select from: MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm).

3 Click **Key**. Enter a passphrase to create a key. Click **OK**.
The passphrase appears in the Authentication Key field. You cannot type a key here directly.

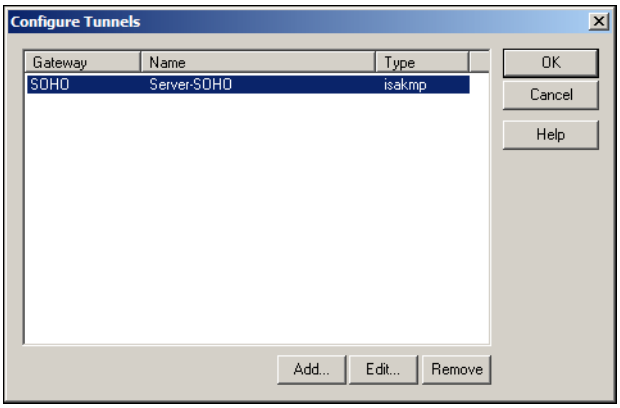
Note

If the two ends of the tunnel are Fireboxes, the remote administrator can also use the encryption and authentication passphrases. If the remote firewall host is an IPSec-compliant device of a different manufacturer, the remote system administrator must use the actual keys. You can see these keys in the dialog box of the Security Association Setup when you set up the remote IPSec-compliant device.

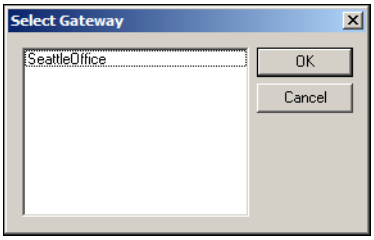
Making a Tunnel with Dynamic Key Negotiation

Use this method to configure a tunnel using a gateway with the Internet Security Association and Key Management Protocol (ISAKMP) key negotiation type. ISAKMP is a protocol to authenticate communication between two devices. This procedure includes the information on how the devices use security services, including encryption. It also includes how to make the keys that you use to change the encrypted data into text.

1 From Policy Manager, select **Network** > **Branch Office VPN** > **Manual IPSec**. Click **Tunnels**.
The Configure Tunnels dialog box appears.



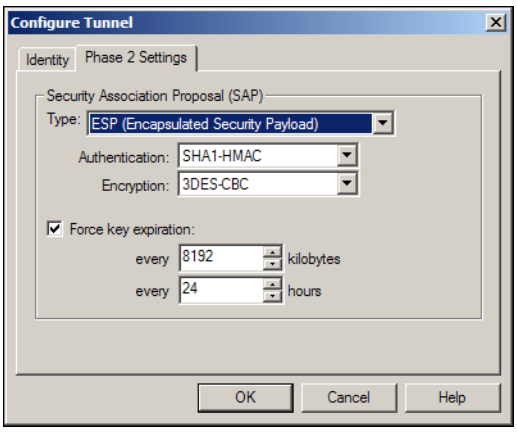
2 Click **Add**.
The Select Gateway dialog box appears.



3 Click a gateway with ISAKMP (dynamic) key negotiation type to connect with this tunnel. Click **OK**.
The Configure Tunnels dialog box appears.

4 Type a tunnel name.
Policy Manager uses the tunnel name to identify it.

5 Click the **Phase 2 Settings** tab.
Use this tab to configure Phase 2 IPSec Security Association properties.



6 From the **Type** drop-down list, select a Security Association Proposal (SAP) type.
Select from: **Encapsulated Security Payload** (ESP) or **Authenticated Headers** (AH).

7 From the **Authentication** drop-down list, select an authentication procedure.
Select from: **None** (no authentication), **MD5-HMAC** (128-bit algorithm), and **SHA1-HMAC** (160-bit authentication algorithm).

8 From the **Encryption** drop-down list, select an encryption procedure.
Select from: **None** (no encryption), **DES-CBC** (56-bit), and **3DES-CBC** (168-bit encryption).

9 To make a new key at specified intervals, select the **Force Key Expiration** check box.
The ISAKMP controller makes and negotiates a new key for the session. For no key expiration, type 0 (zero) here. If you select the Force Key Expiration check box, set the number of kilobytes or the number of hours in the session. Do this before you make a new key to continue the VPN session.

10 Click **OK**.
The Configure Tunnels dialog box appears and shows the new tunnel. Create tunnels until you have finished all tunnels for this gateway.

11 After you add all tunnels for this gateway, click **OK**.
The Configure Gateways dialog box appears.

12 To configure more tunnels for a different gateway, click **Tunnels**. Select a new gateway and create tunnels again for that gateway.

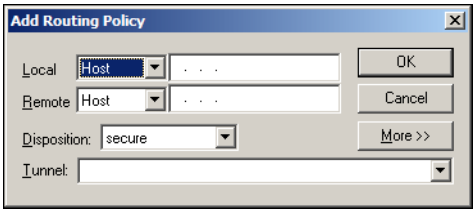
13 When all tunnels are complete, click **OK**.

Making a Routing Policy

Routing policies are sets of rules for how to make outgoing IPSec packets. They also tell if incoming IPSec packets can be accepted. Policies are specified by their endpoints. These are not the same as tunnel or gateway endpoints. Endpoints that set policies are the special hosts or networks that interface through the tunnel. The endpoints are attached to the Fireboxes of the tunnel (or other IPSec-compliant devices).

1 From Policy Manager, select **Network** > **Branch Office VPN** > **Manual IPSec**.
The IPSec Configuration dialog box appears.

2 Click **Add**.
The Add Routing Policy dialog box appears.



3 From the **Local** drop-down list, select a local host or network.

4 Type the IP or network address in slash notation for the local host or network.

5 From the **Remote** drop-down list, select a remote host or network.

6 Type the IP address or network address in slash notation for the remote host or network.

7 From the **Disposition** drop-down list, select a bypass rule for the tunnel:

Secure
IPSec encrypts all traffic that agrees with the rule in related tunnel policies.

Block
IPSec does not give access to traffic that agrees with the rule in related tunnel policies.

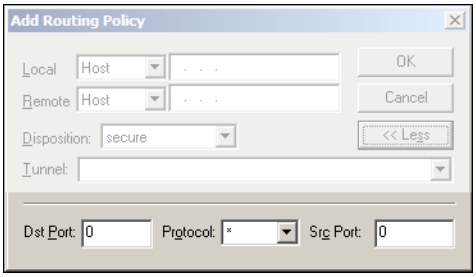
Bypass
IPSec gives access to traffic that agrees with this rule without encryption. This traffic "bypasses" the IPSec routing policy.

Note

If you make a tunnel to a drop-in device with the protection set to Bypass, you must give a host policy for the external IP addresses of the two devices. If not, traffic to and from the external IP address does not match with network policy set for the VPN. Make sure that Bypass policies are at the top of the policy list. Refer to "Changing IPSec policy order" on page 130.

8 When you select **Secure**, use the **Tunnel** drop-down list to select a configured tunnel.
To configure a new tunnel, see "Making a Tunnel with Manual Security" on page 125 or "Making a Tunnel with Dynamic Key Negotiation" on page 127. To show more information about the selected tunnel, select **More**.

9 If necessary, create a limit on the policy to a specified source port, destination port, or protocol. Select **More**.
The text boxes for ports and protocol appear.



10 Type the port number for the remote host in the **Dst Port** text box. Do this to put a limit on the policy to one destination port.
You can select the remote host port number. The port number is the port to which WatchGuard sends traffic for the policy. To enable traffic to all ports, type zero (0).

Note

WatchGuard recommends that you put a limit on the connection ports in Policy Manager, not BOVPN.

11 From the **Protocol** drop-down list, select a value to put a limit on the protocol used by the policy.
Select from: * (specify ports but not protocol), **TCP**, and **UDP**.

12 To control the policy to one source port, type the local host port in the **Src Port** text box.
You can select the local host port number. The port number is the port from which the Firebox sends all traffic for the policy. To enable traffic from all ports, type zero (0).

Note

If you put a limit on the policy to a specified source, port, or protocol, you can accidentally stop traffic.

13 Click **OK**.
The **IPSec Configuration** dialog box appears and shows the new policy. Policies are in the sequence in which they were made. To change the sequence, ***see the subsequent section***.

Configuring routing policies for proxies over VPN tunnels

Connections from BOVPN tunnels to the Internet, with a VPN peer as the default route, are outgoing connections and can be proxied.

From the **IPSec Configuration** dialog box:

1 Click **Add**.
The **Add Routing Policy** dialog box appears.

2 From the drop-down list adjacent to **Local**, select **Network**.

3 Set the IP address as 0.0.0.0/0.

4 From the **Remote** drop-down list, select a remote host or network.

5 Type the IP address or network address in slash notation for the remote host or network.

6 From the **Disposition** drop-down list, select **Secure**.

7 From Policy Manager, add a proxy service. Refer to "Adding a service" on page 44.

8 On the **Properties** tab, click **Outgoing**.

9 Below the **From** list, click **Add**.

10 Click **Network IP Address** and use the address you used for **Remote** in step 5.

11 Below the **To** list, click **Add**.

12 In the Members dialog box, select **External**.

Changing IPSec policy order

The Firebox applies policies in the recorded sequence, from the top down, in the **IPSec Configuration** dialog box. Initially, the policies record as you make them. You must manually arrange the policies from more important to less important. This is to make sure that the routing of sensitive connections goes along the higher-security tunnels. WatchGuard recommends this policy sequence:

- Host to host
- Host to network
- Network to host
- Network to network

Set policies in the same sequence at the two ends of the tunnel.

From the **IPSec Configuration** dialog box:

- To move a policy up in the list, select the policy. Click **Move Up**.
- To move a policy down in the list, select the policy. Click **Move Down**.

Configuring multiple policies per tunnel

If you use two or more policies for a tunnel, the sequence must be the same on each Firebox. For example, Firebox1 and Firebox2 have a tunnel between them and have Policy A and Policy B. For the tunnel to operate, the Fireboxes must have Policy A and then Policy B. If one Firebox has Policy A first and the other has Policy B first, the tunnel will not operate.

If you have more routing policies to a device, each routing policy tunnel must have a special name. For more policies, add a new tunnel. Give it a special name with the same gateway and security adjustments. When you add this routing policy, select the second tunnel name.

Configuring services for BOVPN with IPSec

Access control is a very important part of configuring a secure VPN connection. If a hacker gets access to computers on the branch office VPN network, the attacker can get a secure tunnel to your network.

The Users on the remote Firebox are not in the trusted network. You must configure the Firebox to let traffic through the VPN connection. A fast procedure is to make a host alias that is related to the VPN remote networks and hosts. Then, you can use the host alias or manually type the remote VPN networks and hosts when you configure these service properties:

Incoming

- Enabled and Allowed
- From: Remote VPN network, hosts, or host alias
- To: Trusted or selected hosts.

Outgoing

- Enabled and Allowed
- From: Trusted network or selected hosts
- To: Remote VPN network, hosts, or host alias.

For more information on configuring services, see ***Chapter 8, “Configuring Filtered Services.”***

Let VPN access any service

To let all traffic through from VPN connections, add the Any service to the Services Arena and configure it.

Let VPN access specific services

To let traffic through from VPN connections only for specified services, add each service to the Services Arena and configure them.

Enabling the BOVPN Upgrade

Although the factory default Firebox® X500 does not use BOVPN, you can get a license key to enable this feature. Firebox X700, Firebox X1000, and Firebox X2500 can use BOVPN if you register the device with LiveSecurity® Service.

The BOVPN Upgrade is available from your local reseller. For more information about how to get WatchGuard options, go to:

http://www.watchguard.com/sales/

To enable the BOVPN after you receive your license key:

1 From Policy Manager, click **Setup** > **Firebox Model**. Make sure that **Firebox III/500** or **Firebox X500** is selected.

2 From Policy Manager, click **Network** > **Branch Office VPN** > **Manual IPSec**.
The IPSec Configuration dialog box appears.

3 Click the **License** button.
The IPSec Branch Office License dialog box appears.

4 Type your license key in the text box to the left of the **Add** button. Click **Add**.

CHAPTER 13

Configuring IPSec Tunnels

WatchGuard® System Manager supplies speed and reliability when building IPSec VPN tunnels through drag-and-drop tunnels, an automatic wizard, and the use of templates. You can make fully authenticated and encrypted IPSec tunnels in minutes. You can be sure that they operate with other tunnels and security policies.

From the same interface, you can control and monitor the VPN tunnels. For more information on how to monitor tunnels, see "Monitoring Your Network" in the WatchGuard System Manager User Guide.

System Manager also allows you to safely manage Firebox® X Edge devices from a distance. For more information, see "Managing the Firebox X Edge and Firebox SOHO 6" in the WatchGuard System Manager User Guide.

Steps in making VPNs

- Configure a WatchGuard Management Server and Certificate Authority (CA)
- Add Fireboxes or Firebox X Edge or SOHO devices to the Management Server
- (Dynamic devices only) Configure the Firebox as a Managed Client
- Make policy templates to configure which networks have access through VPN tunnels
- Make security templates to set the encryption type and authentication type
- Make tunnels between the devices.

Management Server

The WatchGuard® Management Server tsoftware is installed on your management station or a different computer. This server replaces the DVCP server that previously operated on the Firebox® X.

Using the new component and management software gives you the ability to:

- Start and stop the Management/CA server
- Set the Management/Certificate Authority (CA) Server passphrases
- Set the Management Server license key
- Set the Management/CA Server diagnostic logging flag
- Set the CA domain name

- Set the CRL distribution point
- Set the CRL publication period
- Set the client certificate lifetime
- Set the root certificate lifetime

WatchGuard Management Server Passphrases

The WatchGuard® Management Server uses a number of passwords to protect sensitive information stored on disk or to secure communications with client systems. After you install the WatchGuard Management Server software, you must run the Configuration Wizard to configure the Management/CA server. This wizard prompts for these passwords:

- Master encryption key
- Management Server passphrase

The management server passphrase and other automatically generated passphrases are stored in a passphrase file.

Master encryption key

The first passphrase that the Configuration Wizard prompts for is the master encryption key. This password is used to protect all the passphrases that are stored in the passphrase file.

The master encryption key is needed so that all the other passphrases that are used are not stored in the clear on disk. If they were, anybody with access to this data (such as on a backup tape) could easily discover the passphrases and use them to get access to other sensitive data on the disk.

Select and store the master encryption key carefully and securely. Use best practices when you select the passphrases. In particular, do not use the same string for the master encryption key and the management server passphrase.

The master encryption key is needed when you:

- Migrate the management server data to a new system
- Restore a lost or corrupt master key file
- Change the master encryption key

Because the master encryption key is not needed frequently, we recommend that you write it down and lock it in a secure location.

Management Server passphrase

The second password that the Configuration Wizard prompts for is the management server passphrase. This passphrase is used frequently by the administrator, because it is the one needed to connect to the Management Server using the WatchGuard System Manager application.

Password and key files

The management server passphrase and all the automatically generated passphrases are stored in a passphrase file. The passphrase data in this file is protected by the master encryption key. The master encryption key itself is not stored on disk. Instead, an encryption key is derived from the master encryption key and the key data is stored on disk.

The default locations for the password file and encryption key are:

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.ini

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.key

Note that these files are used by the Management Server software and must never be modified directly by an administrator.

Microsoft SysKey utility

The password file is protected by the master key. This key is protected by another encryption key, which is protected by the Windows system key.

Windows operating systems use a system key to protect the Security Accounts Management (SAM) database. This is a database of the Windows accounts and passwords on the computer. By default, the system key data is hidden throughout the registry. This allows the system to start without outside intervention--the system key is reassembled from the registry during the startup procedure. Although the system key data is still present on disk, it is not in a form that is easy to get.

If you want a more secure system, you can remove the system key data from the registry so that this particularly sensitive data does not reside on the system at all.

You can use the SysKey utility to:

- Move the system key to a floppy disk
- Require a startup password at boot time
- Move the system key back to the system

If you choose to move the startup key to a floppy disk, then that disk must be inserted in the drive for the system to start. If you choose to require a startup password, an administrator must type in the password each time the system starts.

To configure SysKey options, click **Start > Run**, type **syskey**, and click **OK**.

Setting Up the Management Server

The Management Server Setup Wizard creates a new Management Server on your workstation. It can also migrate an existing Management Server from a Firebox® to a new Management Server on a workstation. For information on moving a Management Server off a Firebox, see the Migration Guide.

If you change the IP address of the Management Server computer, you must remove the Management Server and install it again.

This procedure shows the steps you must follow to successfully set up a new Management Server. Follow this process if you do not currently have a Management Server.

1 Right-click on the Management Server icon in the WatchGuard toolbar on the Windows taskbar.

2 Select **Start Service**.

3 The Management Server Setup Wizard starts. Click **Next**.

4 A master encryption key is required to control access to the WatchGuard management station. Type a passphrase of at least eight characters and then type it again to confirm. Click **Next**.
It is important to remember this passphrase because if you lose it there is no way to recover it.

5 Type the passphrase to use to manage the WatchGuard® Management Server. Click **Next**.
Type a passphrase of at least eight characters and then type it again to confirm.

6 Type the IP address and passphrases for your gateway Firebox. Click **Next**.
The gateway Firebox protects the management server from the Internet.

7 Type the license key for the Management Server. Click **Next**.
8 Type the name of your organization. Click **Next**.
An information screen that lists the details of your server appears.
9 Click **Next**.
The wizard configures the server.
10 When the configuration is complete, click **Finish**.

Adding Devices

You must manually add devices to your Management Server configuration.

Note

Add devices with both static and dynamic IP addresses using this procedure. A device with a dynamic IP address must also be configured as a Managed Client from the Policy Manager for the device.

1 Open WatchGuard System Manager and select **File > Connect to > Server**.
Type the passphrase to connect to your Management Server.
2 From the **VPN** tab, select **Server** > **Insert Device**.
The WatchGuard® Device Wizard appears.
3 Click **Next**.
4 Type a display name for the device.
This is a name that you select. It is not the same as the DNS name of the device.
5 From the **Device Type** drop-down list, select the device type and address method.
A dynamic device must have a dynamic DNS client name.
6 For a static IP address, type the hostname or IP address. For a dynamic IP address, type the client name.
The hostname is the DNS name, not the display name that you defined in step 3.
7 Type the status and configuration passphrases.
8 If you use a device type with a dynamic IP address, type the shared secret. Click **Next**.
9 Type a WINS or DNS server IP addresses and the domain for your configuration. Click **Next**.
If you do not use DNS or WINS servers, ignore this page, and click Next.
The wizard shows the Contact Information page.
10 Select or Add a contact record. This record gives the contact information for this Firebox. Click **Next**.
The information on this page is optional.
11 The wizard then shows a page that gives the subsequent steps. Click **Next**.
When completed, the wizard shows the message New Device Successfully Changed.
12 Click **Close**.
The wizard uploads the new configuration to the Management Server and exits.

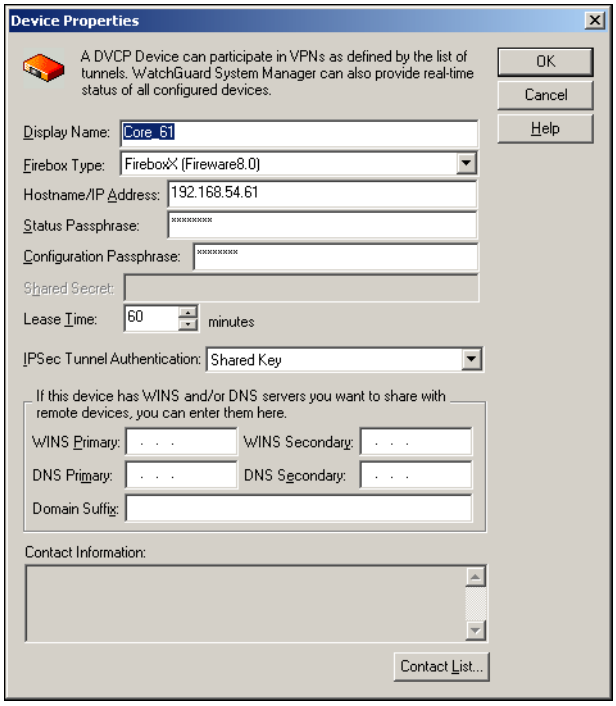
Note

If traffic is heavy and CPU utilization is high, the WatchGuard Device Wizard may occasionally fail because of SSL timeout. Try again later when the system has less load.

Updating a device's settings

You can use the Device Properties dialog box to configure the adjustments of a selected device again.

1 From the **VPN** tab, right-click a device and select **Properties**.
The Device Properties dialog box appears.


Device Properties
A DVCP Device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.
OK
Cancel
Help
Display Name: Core_61
Firebox Type: FireboxX (Fireware8.0)
Hostname/IP Address: 192.168.54.61
Status Passphrase:
Configuration Passphrase:
Shared Secret:
Lease Time: 60 minutes
IPSec Tunnel Authentication: Shared Key
If this device has WINS and/or DNS servers you want to share with remote devices, you can enter them here.
WINS Primary:
WINS Secondary:
DNS Primary:
DNS Secondary:
Domain Suffix:
Contact Information:
Contact List...

2 Change the properties as necessary.

3 Click **OK** when the configuration is complete.

Configuring a Firebox as a Managed Firebox Client (Dynamic Devices only)

To allow WatchGuard System Manager to manage a Firebox, Edge, or SOHO with a dynamic IP address, you must enable it as a managed Firebox client. The instructions here give you the steps to configure a Firebox III or Firebox X as a managed Firebox client. To configure a Firebox X Edge or Firebox SOHO as a managed Firebox client, refer to your Edge or SOHO *User Guide* for information about using the device with managed VPN.

From the Policy Manager for a Firebox III or Firebox X device::

1 Select **VPN > Managed Client.**

2 Select the check box **Enable this Firebox as a Managed Client**.

3 In the **Firebox Name** field, give the name of the Firebox.

4 To log messages for the Managed Client, select the check box **Enable diagnostic log messages for the Managed Client**. (WatchGuard recommends this option only to do troubleshooting).

5 To add management servers that the client can connect to, click **Add**.

6 Type the IP address. Type the shared secret. Click **OK**.

7 Start the Firebox again.
The Firebox connects to the Management Server.

Adding Policy Templates

For a VPN, you can configure (and put a limit to) the networks that have access through the tunnel. You can make a VPN between two hosts or between more networks. To configure the networks available through a given VPN device, you make policy templates. By default, WSM adds and applies a network policy template that gives access to the network behind the VPN device, if the device has a static IP address.

Get the latest templates from a device

Before you add more policy templates, get the latest templates from the device. This is most important for dynamic devices because the Firebox automatically adds a network policy template for static devices Before you update a device, make sure that it has is configured as a managed Firebox client.

1 In WatchGuard System Manager, select a managed client and click **Server > Update Device**.

2 select **Download Trusted and Optional Network Policies**.

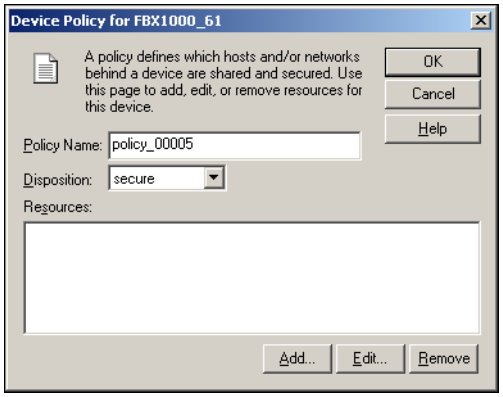
3 Click **OK**.

Make a new policy template

To make a policy template, on the **VPN** tab:

1 Select the device for which to configure a policy template.

2 Right-click and select **Insert Policy** or click the Insert Policy Template icon.
The Device Policy dialog box for that device appears.



3 Type a policy name.

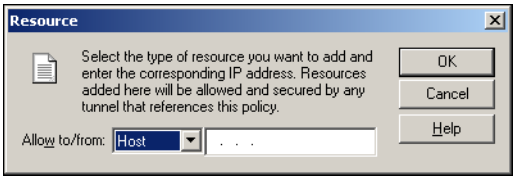
4 Select the actions for this policy. A policy can secure resources, block resources, or bypass resources. Use bypass if the resource is not affected by the tunnel. Use block if the tunnel clients cannot access the resource. Use secure if the tunnel resource is to be shared securely with tunnel clients.

5 Add, edit, or delete resources from the tunnel policy. Click **Add** to to add an IP address or a network address to the tunnel policy. Click **Edit** to edit a resource that you have selected in the list. Click **Remove** to delete a resource you have selected in the list.

6 Click **OK**.
The policy template is configured and is available in the VPN configuration area.

Adding resources to a policy template

1 From the **Device Policy** dialog box, click **Add**.
The Resource dialog box appears, see the figure that follows.


Resource
Select the type of resource you want to add and enter the corresponding IP address. Resources added here will be allowed and secured by any tunnel that references this policy.
OK
Cancel
Help
Allow to/from:
Host

2 Select the type of resource and give its IP or network address. Click **OK**.

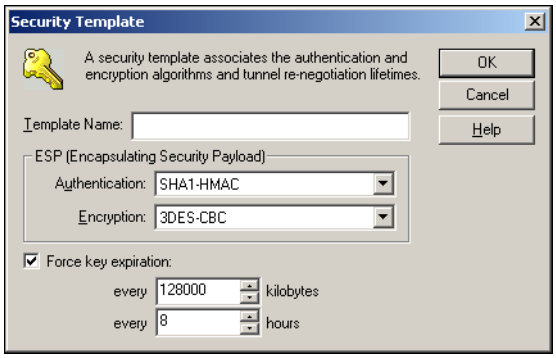
Adding Security Templates

A security template gives the encryption type and authentication type for a tunnel.

Default security templates are supplied for the available encryption types. You can also make new templates. Security templates make it easy to set the encryption type and authentication type with the tunnel from the Configuration wizard.

To make a policy template, on the **VPN** tab:

1 Right-click in the window, and select **Insert Security Template** or click the Insert Security Template icon (shown at the right side).
The Security Template dialog box appears, see the figure that follows.



2 Type the template name. Select the authentication method, and encryption.

3 To get end dates for a key, select the related check box, and then give kilobytes, hours, or the two.
If you give two values, the key stops at the event that comes first.

The security template is configured. You can select it in the VPN Wizard when you make a VPN tunnel with that device.

4 Click **OK**.

Making Tunnels Between Devices

You can configure a tunnel with the drag-and-drop procedure or the Add VPN Wizard.

Drag-and-drop tunnel procedure

To use the drag-and-drop tunnel procedure, dynamic Fireboxes and Firebox X Edge or SOHO devices must have networks that are configured before you can use this procedure. You must also get the policies from any new dynamic devices before you configure drag-and-drop tunnels (use the procedure "Get the latest templates from a device" on page 138 to do this).

On the VPN tab:

1. Click the device name of one of the tunnel endpoints. Drag it to the device name of the other tunnel endpoint.
   This starts the Add VPN Wizard.
2. Click **Next** to pass the introduction screen.
3. The gateway devices screen shows the two endpoint devices you selected with drag-and-drop, and the policy templates that the tunnel uses. If necessary, select the devices for the endpoints of the tunnel.
4. For each device, select a policy template from the drop-down list.
   The policy template configures the resources available through the tunnel. Resources can be a network or a host. The pull-down list shows the policy templates that you added to VPN Manager.
5. Click **Next**.
   The wizard shows the Security Policy dialog box.
6. Select the security template applicable for the type of security and type of authentication to use for this tunnel.
   The listbox shows the templates you added to the Management server.
7. Click **Next**.
   The wizard shows the configuration.
8. Select the checkbox **Restart devices now to download VPN configuration**. Click **Finish** to start the devices again and deploy the VPN tunnel.

Using the Add VPN Wizard without drag-and-drop

To create tunnels using the Add VPN Wizard without drag-and-drop:

1. From the VPN tab, select **Server** > **Create a new VPN** or click the Create New VPN icon (shown at the right).

   This starts the Add VPN Wizard.
2. Click **Next**.
   The wizard shows two listboxes that each list all the devices registered in the Management Server.
3. Select a device from each list box to be the endpoints of the tunnel you make.
4. Select the policy templates for the end of the tunnel of each device.
   The listbox shows the templates added to the Management Server.
5. Click **Next**.
   The wizard shows the Security Template dialog box.
6. Select the applicable security template for this VPN. Click **Next**.
   The wizard shows the configuration.
7. Select the check box **Restart devices now to download VPN configuration**. Click **Finish** to start the devices again and deploy the VPN tunnel.

Editing a Tunnel

You can see all your tunnels on the **VPN** tab of WatchGuard® System Manager. System Manager lets you change the tunnel name, security template, endpoints, and the policy used.

On the **VPN** tab:

1 Expand the tree to show the device and its policy to change.

2 Highlight the tunnel to change.

3 Right-click and select **Properties**.
The Tunnel Properties dialog box appears.

4 Click **OK** to save the change.
When the tunnel is renegotiated, the changes are applied.

Removing Tunnels and Devices

To remove a device from WatchGuard® System Manager, you must first remove the tunnels for which that device is an endpoint.

Removing a tunnel

1 From System Manager, click the **VPN** tab.

2 Expand the **Managed VPNs** folder to show the tunnel to remove.

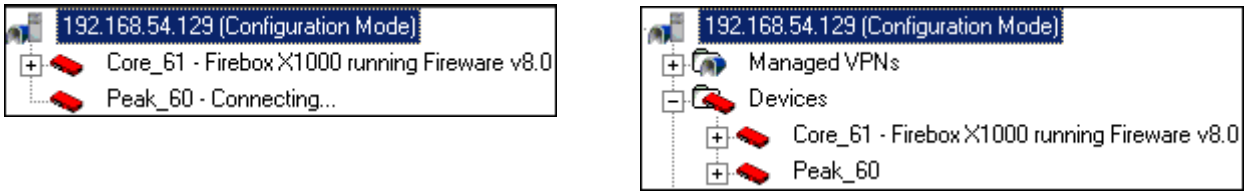
3 Right-click the tunnel.

4 Select **Remove**. Click **Yes**. to confirm

5 If necessary, give a start again command to the devices from this removal, click **Yes**.

Removing a device

1 From System Manager, click the **Device** or **VPN** tab.
The Device tab (left side figure below) or the VPN tab (right side figure below) appears.



Device tab (left side) and VPN tab (right side)

2 If you use the **VPN** tab, expand the **Devices** folder to show the device to remove.

3 Right-click the device.

4 Select **Remove**. Click **Yes** to confirm.

CHAPTER 14

Configuring RUVPN with PPTP

Remote User Virtual Private Networking (RUVPN) uses Point-to-Point Tunneling Protocol (PPTP) to make a secure connection. It gives support to 50 users at the same time for each Firebox® and operates with all types of Firebox encryption. RUVPN users can authenticate to the Firebox or to a RADIUS authentication server. You must configure the Firebox and the remote host computers of the RUVPN user.

Configuration Checklist

Before you configure a Firebox® to use RUVPN, record this information:

- The IP addresses for the remote client during RUVPN sessions. **These IP addresses cannot be addresses that the network behind the Firebox uses.** The safest procedure to give addresses for RUVPN users is to install a "placeholder" secondary network with a range of IP addresses. Then, select an IP address from that network range. For example, create a new subnet as a secondary network on your trusted network 10.10.0.254/24. Select 10.10.0.0/27 for your range of PPTP addresses.
- The IP addresses of the DNS and WINS servers that resolve IP addresses to host alias names.
- The user names and passwords of users that are approved to connect to the Firebox with RUVPN.

Encryption levels

Because of export limits on high encryption software, WatchGuard® Firebox products are put on the installation CD-ROM with only base encryption.

For RUVPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. U.S. domestic versions of Windows XP have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows. The Firebox always tries to use 128-bit encryption first. It uses (if enabled) 40-bit encryption if the client cannot use the 128-bit encrypted connection.

For information on how to enable the drop to 40-bit, see "Activating RUVPN with PPTP" on page 147. For more information about encryption and PPTP tunnels, see the FAQ:

https://www.watchguard.com/support/AdvancedFaqs/pptp_tunnelencryp.asp

If you do not live in the U.S. and you must have strong encryption on your LiveSecurity® Service account, send an e-mail to supportid@watchguard.com and include in it:

- Your LiveSecurity Service key number
- Date of purchase
- The name of your company
- Company mailing address
- Telephone number and name
- E-mail address to reply to.

If you live in the U.S., you must download the strong encryption software from your archive page in the LiveSecurity Service Web site. Go to www.watchguard.com, click **Support**, log into your LiveSecurity Service account, and then click **Latest Software**.

Then, uninstall the initial encryption software, and install the strong encryption software from the downloaded file.

Note

To keep your current Firebox configuration, do not use the Quick Setup Wizard when you install the new software. Open System Manager, connect to the Firebox, and save your configuration file. Configurations with a different encryption version are compatible.

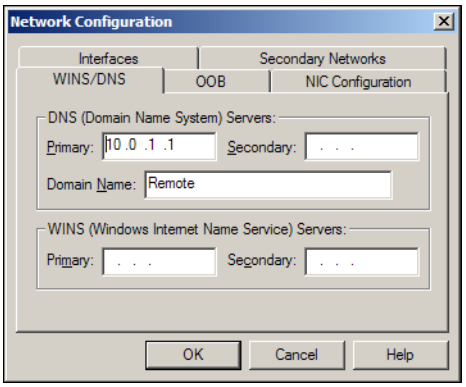
Configuring WINS and DNS Servers

RUVPN clients use shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS changes host names into IP addresses, while WINS changes NetBIOS names to IP addresses. The trusted interface of the Firebox® must have access to these servers.

Make sure that you use an internal DNS server. Do not use external DNS servers.

From Policy Manager:

1 From Policy Manager, click **Network** > **Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears.



2 In the **Primary** and **Secondary** text boxes, type the primary and secondary addresses for the WINS and DNS servers. Type a domain name for the DNS server.

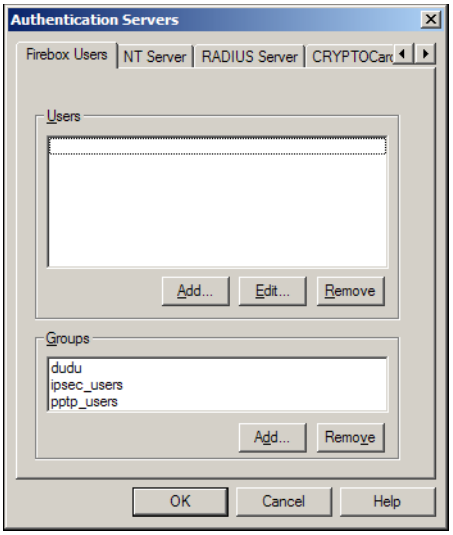
Adding New Users to Authentication Groups

You can use the Firebox® or a RADIUS server to authenticate users for RUVPN with PPTP. Put all RUVPN users in the built-in Firebox authentication group, the pptp_users. This group contains the user names and passwords of RUVPN users. Use this group to configure the services for incoming traffic.

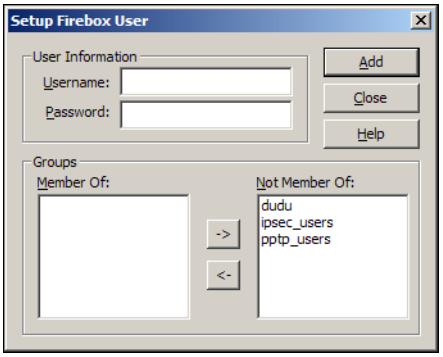
To get access to Internet services (such as outgoing HTTP or outgoing FTP), the remote user gives a user name and password as authenticating data. The WatchGuard© System Manager software uses this information to authenticate the user to the Firebox.

For more information on Firebox groups, see "Creating Aliases and Implementing Authentication," on page 93.

1 From Policy Manager, click **Setup** > **Authentication Servers**.
The Authentication Servers dialog box appears.



2 To add a new user, click the **Add** button below the **Users** list.
The Setup Firebox Users dialog box appears.



3 Type a user name and password for the new user.

4 Select **pptp_users** in the **Not Member Of** list. Then click the arrow to move the name to the **Member Of** list. Click **Add**.
The new user is put on the User list. The dialog box of the Setup Remote User stays open and you can add more users.

5 To close the **Setup Remote User** dialog box, click **Close**.
The Firebox Users tab appears with a list of the new configured users.

6 When all the new users are on the list, click **OK**.
You can use the users and groups to configure the services. Refer to the subsequent section.

Configuring Services to Allow RUVPN Traffic

RUVPN users have no access privileges through a Firebox®. You must add user names or the full pptp_users group to service icons in the Services Arena. This gives remote users access to machines behind the Firebox.

WatchGuard® recommends two procedures to configure the services for RUVPN traffic: an individual service and the Any service. The Any service "opens a hole" through the Firebox, this lets all the traffic flow between hosts without applying firewall rules.

By individual service

In the Services Arena, double-click a service to enable for your VPN users. Set the properties that follow on the service:

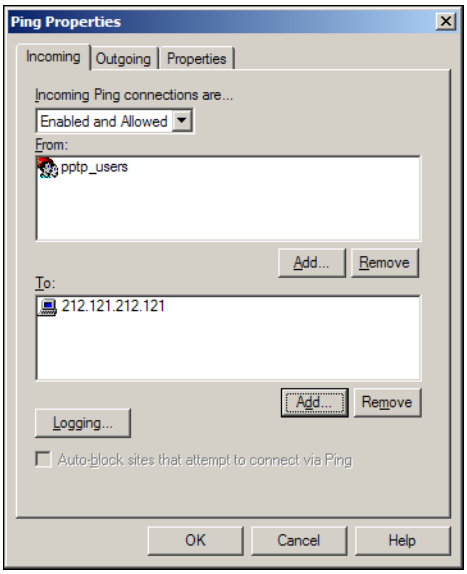
Incoming

- Enabled and allowed
- From: pptp_users
- To: trusted, optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted, optional, network or host IP address, or alias
- To: pptp_users

An example of how you can set the incoming properties for a service appears on the figure that follows.



Using the Any service

Add the Any service with these properties:

Incoming

- Enabled and allowed
- From: pptp_users

- To: trusted, optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted, optional, network or host IP address, or alias
- To: pptp_users

Make sure that you save your configuration file to the Firebox after you make these changes.

Note

To use WebBlocker to control the access of remote users, add pptp_users to a proxy service that controls WebBlocker, such as Proxied-HTTP. Use this as an alternative to the Any service.

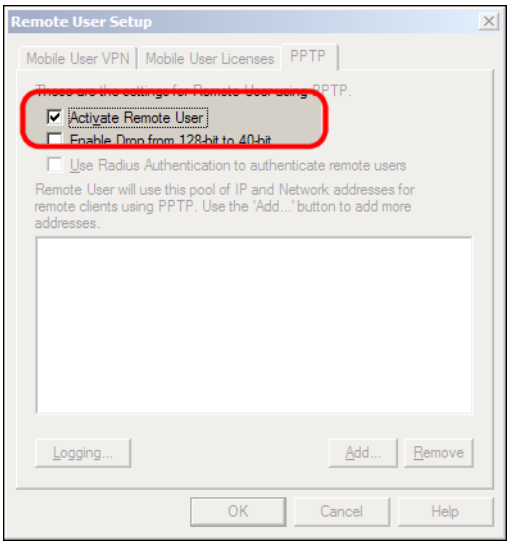
Activating RUVPN with PPTP

To configure RUVPN with PPTP you must enable the feature. RUVPN with PPTP adds the wg_pptp service icon to the Services Arena. This sets default properties for PPTP connections and for the traffic that flows to and from them. WatchGuard® recommends you do not change the default properties of the wg_pptp service.

1 From Policy Manager, click **Network** > **Remote User**. Click the **PPTP** tab.

2 Select the **Activate Remote User** check box.

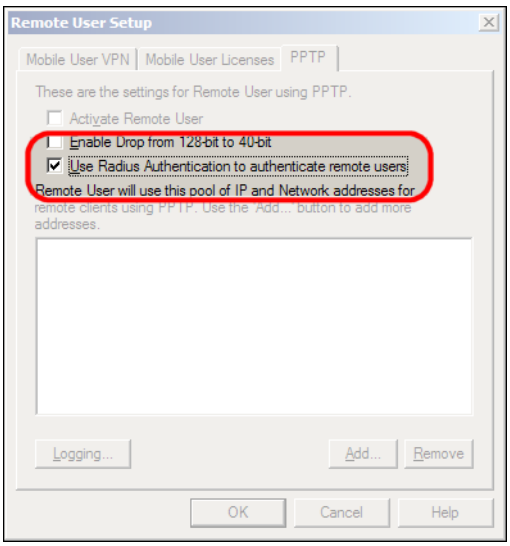
3 If necessary, select the **Enable Drop from 128-bit to 40-bit** check box.
Usually, only customers outside the United States use this check box.



Enabling Extended Authentication

RUVPN with extended authentication lets users authenticate to a RADIUS authentication server as an alternative to the Firebox®. For more information on extended authentication, see the *WatchGuard System Manager User Guide* introduction to virtual private networking.

1 Select the **Use RADIUS Authentication to authenticate remote users** check box.



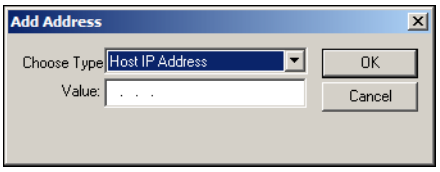
2 Configure the RADIUS server with the **Authentication Servers** dialog box. Refer to Chapter 10, "Creating Aliases and Implementing Authentication."

3 On the RADIUS server, add the user to the pptp_users group.

Entering IP Addresses for RUVPN Sessions

RUVPN with PPTP gives support to 50 users at the same time, although you can configure a much larger number of client computers. The Firebox gives an open IP address to each incoming RUVPN user from a group of available addresses. This goes on until all the addresses are in use. After the user closes a session, the address is put back in the available group. The subsequent user who logs in gets this address.

1 From the **PPTP** tab on the dialog box of the **Remote User Setup** dialog box, click **Add**.
The Add Address dialog box appears.



2 From the **Choose Type** drop-down list, select a host or a network.
You can configure 50 addresses. If you select a network address, RUVPN with PPTP uses the first 50 addresses in the subnet.

3 In the **Value** text box, type the host or network address in slash notation. Click **OK**.
Type IP addresses that are not in use which the Firebox can give to clients during RUVPN with PPTP sessions. The IP address appears in the list of addresses available to remote clients.

4 Do the procedure again to configure all the addresses for use with RUVPN with PPTP.

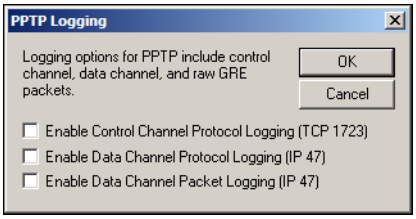
Configuring Debugging Options

WatchGuard® gives a selection of logging options you can set to collect information and aid with troubleshooting. These debugging options can increase the log message volume, which can have an effect on Firebox® performance. WatchGuard recommends you use them only to troubleshoot RUVPN problems.

1 From Policy Manager, click **Network** > **Remote User**.
The Remote User Setup window appears with the Mobile User VPN tab selected.

2 Click the **PPTP** tab.

3 Click **Logging**.
The PPTP Logging dialog box appears.


PPTP Logging
Logging options for PPTP include control channel, data channel, and raw GRE packets.
OK
Cancel
Enable Control Channel Protocol Logging (TCP 1723)
Enable Data Channel Protocol Logging (IP 47)
Enable Data Channel Packet Logging (IP 47)

4 Click the logging options to start.
To see the function of each option, right-click it, and then click What's This?

5 Click **OK**. Save the configuration file to the Firebox.

Preparing the Client Computers

You must first prepare each computer that you use as an RUVPN with PPTP remote host, with:

- Internet service provider (ISP) account
- Public IP address.

After you install these items, do the procedures in this section:

- Install the necessary version of Microsoft Dial-Up Networking and the necessary service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not necessary for all operating systems).

Installing MSDUN and Service Packs

It can be necessary to install these options for correct configuration of RUVPN:

- MSDUN (Microsoft Dial-Up Networking) upgrades
- other extensions
- service packs.

For RUVPN with PPTP, it is necessary to install these upgrades:

Encryption	Platform	Application
Base	Windows NT	40-bit SP4

Encryption	Platform	Application
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2

*40-bit encryption is the default for Windows 2000. If you upgrade from Windows 98, with strong encryption, Windows 2000 will automatically set strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center Web site at:

www.microsoft.com/downloads/search.asp

Creating and Connecting a PPTP RUVPN on Windows XP

To prepare a Windows XP remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1. Click **Start** > **Control Panel** > **Network Connections**.
   The Network Connection wizard appears.
2. Click **Create a new connection** from the menu on the left. The New Connection Wizard starts. Click Next.
3. Click **Connect to the network at my workplace**. Click **Next**.
4. Click **Virtual Private Network Connection**. Click **Next**.
5. Give the new connection a name, such as "Connect with RUVPN." Click **Next**.
6. Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection. Click **Next**.
   The wizard includes this screen if you are using Windows XP SP2. Not all Windows XP users see this screen.
7. Type the host name or IP address of the Firebox external interface. Click **Next**.
8. Select who can use this connection profile. Click **Next**.
9. Select **Add a shortcut to this connection to my desktop**. Click **Finish**.
10. To connect using your new VPN connection, first make an Internet connection through a dial-up network, or directly through a LAN or WAN.
11. Double-click the shortcut to the new connection on your desktop.
    Or, select **Control Panel** > **Network Connections** and look under the Virtual Private Network list for the connection you created.
12. Type the user name and password for the connection.
    This information was given when you added the user to the pptp_users group. See "Adding New Users to Authentication Groups" on page 145.
13. Click **Connect**.

Creating and Connecting a PPTP RUVPN on Windows 2000

To prepare a Windows 2000 remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1. Click **Start** > **Settings** > **Network Connections** > **Create a New Connection**.
   The New Connection wizard appears.

2 Click **Next**.

3 Select **Connect to the network at my workplace**. Click **Next**.

4 Click **Virtual Private Network connection**.

5 Give the new connection a name, such as "Connect with RUVPN." Click **Next**.

6 Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection. Click **Next**.

7 Type the host name or IP address of the Firebox external interface. Click **Next**.

8 Select **Add a shortcut to this connection to my desktop**. Click **Finish**.

9 To connect using your new VPN connection, first make an Internet connection through a dial-up network, or directly through a LAN or WAN.

10 Double-click the shortcut to the new connection on your desktop.
Or, select **Control Panel > Network Connections** and look under the Virtual Private Network list for the connection you created.

11 Type the user name and password for the connection.
This information was given when you added the user to the pptp_users group. See "Adding New Users to Authentication Groups" on page 145.

12 Click **Connect**.

Running RUVPN and Accessing the Internet

You can enable remote users to get access to the Internet through a RUVPN tunnel. But this option has an effect on security.

1 When you set up your connection on the client computer, edit the **Advanced TCP/IP Settings** dialog box to select the **Use default gateway on remote network** check box.
To open the Advanced TCP/IP Settings dialog box on Windows XP or Windows 2000, right-click on the VPN connection in Control Panel > Network Connections. Select Properties and click on the Network tab. Find Internet Protocol in the list box and click Properties. On the General tab, click Advanced.

2 On the Firebox, make a dynamic NAT entry from VPN to external. To make sure that only some PPTP users can do this, make entries from <virtual IP address> to External.

3 Configure your Outgoing service to let outgoing connections from PPTP-Users to the external interface. If you use WebBlocker to control remote user Web access, add PPTP-Users to the service that controls WebBlocker (like HTTP-Proxy).

Making Outbound PPTP Connections From Behind a Firebox

If necessary, you can make a PPTP connection to a Firebox from behind a different Firebox. For example, a remote user goes to a customer office that has a Firebox. The user can make PPTP connections to their network with PPTP. For the local Firebox to correctly use the outgoing PPTP connection, a PPTP service must be set up as follows:

1 Add the PPTP service. (For information on enabling services, see Chapter 8, "Configuring Filtered Services.")

2 Click **Setup** > **NAT**, and make sure the check box **Enable Dynamic NAT** is selected. This is the default parameter for a Firebox in routed mode.

PART IV Extending Your Protection with Options

CHAPTER 15

Controlling Web Site Access with WebBlocker

The WebBlocker feature of the WatchGuard® System Manager uses the HTTP proxy to apply a filter to the Web. You can control the access to Web sites. You can select the hours in the day that users can get access to the Web. You can also select the category of Web sites that users cannot go to.

For more information on WebBlocker, browse to our Web site at:

www.watchguard.com/products/webblock.asp

You can also route MUVPN and RUVPN with PPTP users through the outgoing HTTP proxy.

Getting Started with WebBlocker

Installation of WebBlocker and the database download is completed with your WatchGuard System Manager installation. See the *WatchGuard System Manager User Guide* for information on installing WebBlocker, installing a WebBlocker license, and downloading the WebBlocker database.

Add an HTTP Service

To use WebBlocker, add the Proxied-HTTP, Proxy, or HTTP service. WatchGuard recommends that you use Proxied-HTTP, which puts a filter on all the ports. HTTP without the Proxy service manages only port 80. WebBlocker overrides the other configurations in the HTTP- or Proxy-services. Thus, you prevent all Web access if you set WebBlocker to "Block All URLs". For information on how to add an HTTP proxy service, refer to "Adding a proxy service for HTTP" on page 80.

Configuring the WebBlocker Service

The services of WebBlocker include HTTP, Proxied HTTP, and Proxy. After you install WebBlocker and add the WebBlocker license, five tabs appear in the Properties dialog box:

- WebBlocker Controls
- WB: Schedule
- WB: Operational Privileges

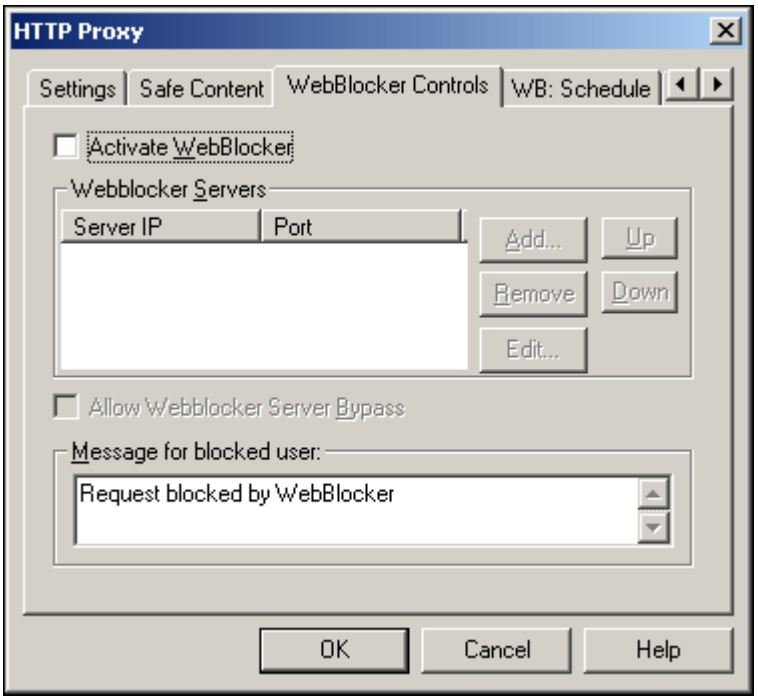
- WB: Non-operational Privileges
- WB: Exceptions.

Activating WebBlocker

From Policy Manager:

1 From Policy Manager, double-click the service icon that you use for HTTP. Click the **Properties** tab.

2 Click **Settings**. Then click the **WebBlocker Controls** tab.



3 Select the **Activate WebBlocker** check box.

4 Adjacent to the **WebBlocker Servers** box, click **Add**.
A dialog box appears.

5 In the **Value** text box, type the IP address of the server. Click **OK**.
If it is necessary to add more WebBlocker servers, refer to "Installing Multiple WebBlocker Servers" on page 160.

Allowing WebBlocker server bypass

Outbound HTTP traffic is automatically denied when the WebBlocker server does not respond. To let all the outbound HTTP traffic through when a WebBlocker server cannot be found, select **Allow WebBlocker Server Bypass on the WebBlocker Controls tab**. This selection is global. If you set it in one HTTP service, it applies to all other HTTP proxy services.

Configuring the WebBlocker Message

You can give the text that appears when the end user tries to open a blocked Web site. You can do this in the field **Message for blocked user.**

The text cannot contain HTML or the greater than (>) and less than (<) characters. You can use these meta-characters:

%u

The full URL of the denied web site.

%s

The block status, or the cause that the web site was blocked. The status can be: **host**, **host/directory**, **all web access blocked**, **denied**, **database not loaded**.

%r

The WebBlocker category or categories that causes the block.

For example, this entry in the field show the URL, the status, and the category:

```
Request for URL %u denied by WebBlocker: %s blocked for %r.
```

With this entry in the **Message for blocked user** field, this text can appear in the browser of an user:

```
Request for URL www.badsite.com denied by WebBlocker: host blocked for violence/profanity.
```

Scheduling operational and non-operational hours

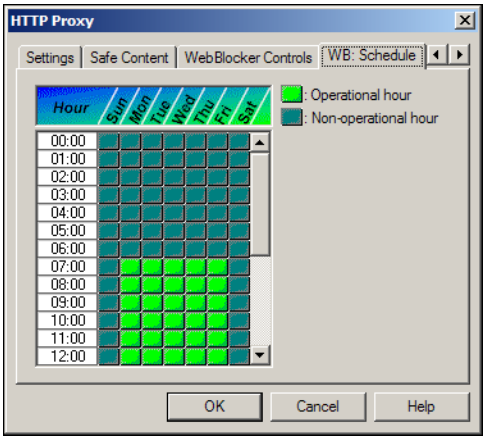
With WebBlocker you can configure two different time periods:

- Operational hours - The usual hours of operation
- Non-operational hours.

You can use these time periods to make the rules about when you block different Web sites.

For example, you can block sports Web sites in the usual hours of operation, and have access at lunch time, evenings, and weekends.

1 From the HTTP Proxy dialog box, click the **WB: Schedule** tab.
The tab appears.



2 Click the hour boxes to identify the time period as an **Operational hour or Non-operational hour.**

Note

The operational and non-operational hour periods change when you set a different time zone. The default WebBlocker configuration is GMT unless you set a Firebox time zone. For more information on how to set the Firebox time zone, refer to “Setting the Time Zone” on page 37.

Setting privileges

Setting privileges

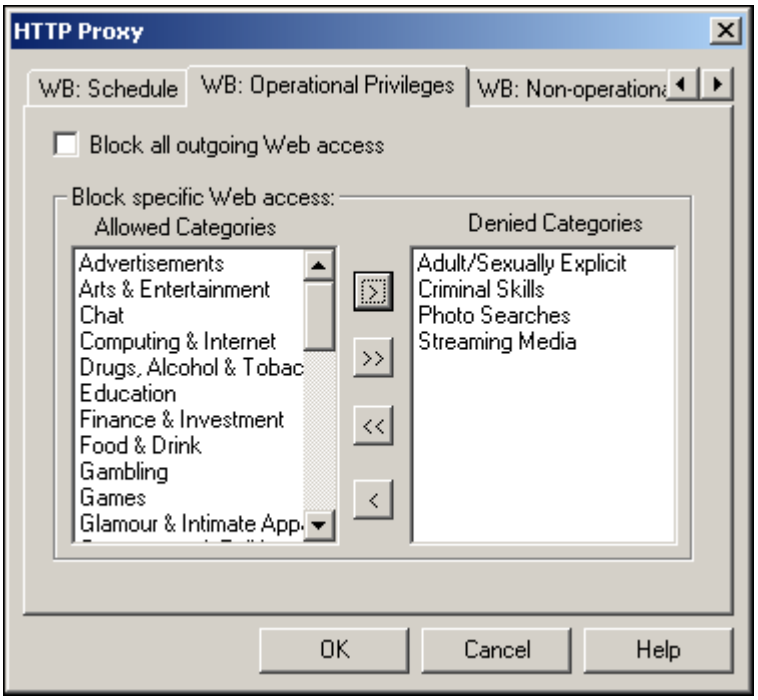
The WebBlocker uses content to identify an URL. Use the Privileges tab to select the type of content access during operational and non-operational hours.

From the proxy dialog box:

1 Click the **WB: Operational Privileges** tab or the **WB: Non-operational Privileges** tab.

2 Select the content types in the **Allowed Categories** list that you want to block, then click the **>** button to add them to the **Denied Categories** list. To deny all categories, click the **>>** button. To move a site from the **Allowed Categories** list to the **Denied Categories** list, click the **<** button. To allow all categories, click the **<<** button.

.



Creating WebBlocker exceptions

You can override a WebBlocker rule with an exception. You can add a Web site that is allowed or denied. The recorded web sites apply only to the HTTP traffic. They are not related to the Blocked Sites list.

The exceptions tool keeps a list of IP addresses that are allowed or denied. You can give exceptions by domain name, network address, or host IP address.

You can also specify a port number, path name, or string which must be blocked for a special Web site. For example, if it is necessary to block only www.sharedspace.com/~dave, because the site of Dave contains nude photographs, you type "~dave" to block that directory of sharedspace.com. This gives the users access to www.sharedspace.com/~julia, which contains a piece on increased production.

If it is necessary to block sexually explicit content that is on sharedspace.com, you can type `*sex`. This blocks a Web page such as www.sharedspace.com/~george/sexy.htm. If you type an asterisk (*) in front of the text, it finds that string anywhere in the URL. If you type *sex in the pattern section, this does not

block all the URLs with the word "sex." The * character only changes the exceptions in a specified URL. For example, if you block www.sharedspace.com/*sex, this blocks www.sharedspace/sexsite.html.

Note

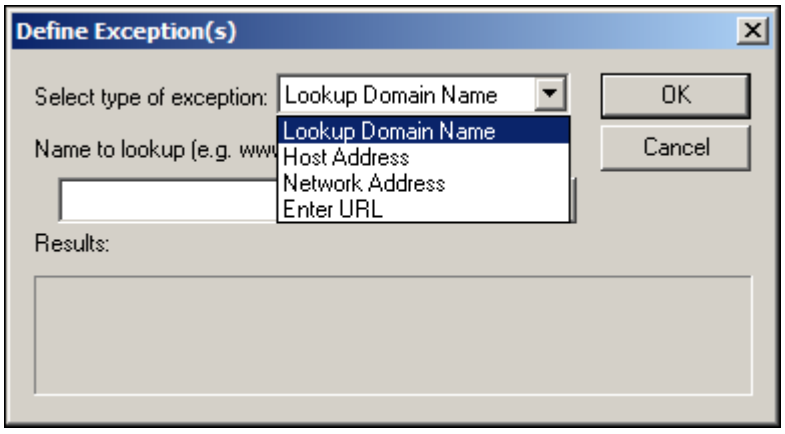
This WebBlocker tool is applicable only when you get access to an external Web site. You cannot use WebBlocker exceptions for an internal host.

From the **HTTP Proxy** dialog box:

1 Click the **WB: Exceptions** tab (if you do not see this tab, use the arrow keys at the right of the dialog box).

2 In the **Allowed Exceptions** section, click **Add**.
The Define Exceptions dialog box appears.

3 From the **Select type of exception** drop-down list, select host address, network address, or type the URL. You can also use the selection **Lookup Domain Name** to find the IP address of a domain.
If you use Lookup Domain Name, the IP addresses that the lookup finds are automatically added to the list after you click **OK**.



4 Type the port or string to let a specified port or directory pattern through.
When you type an IP addresses, type all the numbers and the stops. Do not use the TAB or arrow key. For more information on entering the IP addresses, refer to "Enter the IP addresses" on page 25.

5 In the **Denied Exceptions** section, click **Add**. You must give the host address, network address, or URL.
To block a specified string for a domain, select Host Address. To block a specified directory pattern, type the text (for example, "*poker").

6 To remove an item from the Allow or the Deny list, select the address, and then click **Remove**.

Managing the WebBlocker Server

The WebBlocker server is installed as a Windows service. You can start or stop the service from the WatchGuard toolbar. Right-click the WebBlocker Service icon. Select **Stop Service** or **Start Service**. See the *WatchGuard System Manager User Guide* for more information on the WebBlocker service and the WatchGuard toolbar.

Installing Multiple WebBlocker Servers

You can install two or more WebBlocker servers in a failover configuration. If the primary WebBlocker server fails, the Firebox® automatically fails over to the first server in the WebBlocker Servers box. Refer to "Activating WebBlocker" on page 156.

To add more WebBlocker servers:

1 Open the HTTP Proxy Properties dialog box. Click **Properties**. Click **Settings**.
The HTTP Proxy dialog box appears.

2 Click the **WebBlocker Controls** tab.

3 Click **Add**.
The WebBlocker Server IP dialog box appears.

4 In the **Value** text box, type the IP address of the server. Click **OK**.

You can use the Up and Down buttons to change the position of the servers in the list. When you operate two or more WebBlocker servers in a failover mode, the time between failovers can be as long as two minutes.

CHAPTER 16

Maintaining Connectivity with High Availability

The WatchGuard® High Availability upgrade enables the installation of two Fireboxes on one network in a failover configuration with one Firebox® in active mode and the other in standby mode. The standby Firebox activates when the active Firebox goes off line. After a Firebox becomes active, it stays active until it goes off line and the standby Firebox starts as the active unit. The two Fireboxes in a High Availability pair must have the same configuration file. High Availability is easy to set up and makes sure that your network firewall stays in operation.

Note

In this User Guide, the word Firebox refers to a Firebox® III or a Firebox® X hardware device unless we tell you differently. Illustrations of Fireboxes are interchangeable unless we tell you differently.

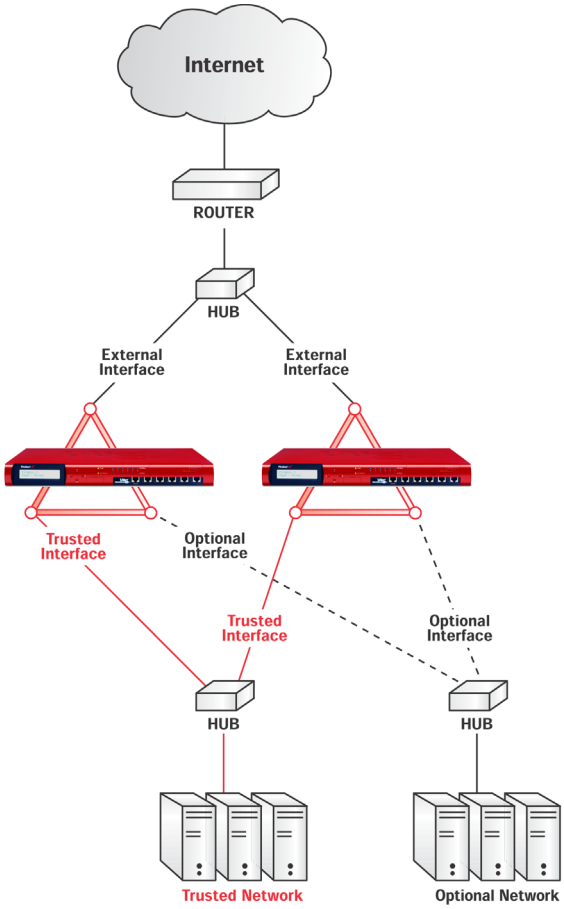
The High Availability Failover Process

To create a High Availability pair, you must have two Firebox® devices that are the same model. One is the active Firebox and the other is the standby Firebox. The relationship between the active Firebox and the standby Firebox is dynamic. When the Firebox starts, it becomes the standby Firebox. If it can not find a matching active Firebox, it changes to become the active Firebox. If two Firebox devices start at the same time, they negotiate active and standby status.

If both of the Firebox devices are active and connected to the network, the Firebox with the longest uptime restarts in standby mode. This is referred to as *High Availability stand down*.

Each Firebox must use the same method to connect to the network. For example, if the external interface of the first Firebox connects to a hub or switch, then you must connect the external interface of the second Firebox to the same hub or switch. Repeat for each Firebox interface.

This figure shows a network with a High Availability pair:



You can use any Firebox interface for the High Availability connection between the two Firebox devices. The default configuration uses the trusted interfaces. The standby Firebox must use a reserved IP address on the same subnet as the High Availability interface on the active Firebox. This allows the active Firebox and the standby Firebox to send and receive connection information:

- Broadcast UDP packets which are known as *High Availability heartbeats*
- TCP connection state information

The standby Firebox sends out ARP packets on the network at a five second interval. These packets request the MAC address of the active Firebox. Then the active Firebox replies with its MAC address. If the standby Firebox does not receive two consecutive responses, it thinks the active Firebox is off line. The standby Firebox then goes to active mode. It starts with the last known TCP connection information sent by the off line Firebox.

Note

Because the heartbeat is a Layer 2 broadcast, a switch or other device that operates between the two Firebox heartbeat interfaces must send and receive Layer 2 broadcasts. WatchGuard recommends that the heartbeat interfaces are connected with a hub, and not a switch, for this reason. See your switch documentation to see if it allows Layer 2 broadcasts.

The *TCP connection state information* is the most current information about the TCP connections on the active Firebox. The standby Firebox requests the TCP connection state information from the active Firebox. The active Firebox sends this data on TCP port 4105.

The two Firebox devices in a High Availability pair must have the same configuration. To put a new configuration file on to the pair:

The management station must have a connection to each Firebox. The management station must also be on the same subnet as the interfaces that the Firebox devices use for High Availability.

First, save the configuration file to the management station before you save the file to the Firebox devices. If you try to upload a configuration file directly from a public folder on a network, the file only goes on the active Firebox.

Installing High Availability

When you buy the High Availability upgrade, you receive a certificate. Use the instructions on the certificate to go to the LiveSecurity® Service web site and activate your upgrade. After you activate the upgrade, you get a High Availability license key. You must add a unique High Availability license key to each Firebox in the High Availability pair. Each Firebox® in the pair have the same version of WatchGuard System Manager software and firmware. You must install the same upgrades on the primary Firebox and the secondary Firebox.

Note

The Firebox X models use a different installation procedure than the Firebox III models. This is because Firebox X license keys are associated with the unit serial number.

You must add all the license keys for the primary Firebox X and the secondary Firebox X to the configuration file. This allows each Firebox in the pair to use all of the options you have when it becomes the active Firebox. Thus, for each upgrade you enable, you enter two license keys into the Firebox X configuration file: one for the primary Firebox and one for the secondary Firebox. For more information, go to the LiveSecurity Service web site.

Most of the options you purchase for a Firebox X are copied to the standby unit when LiveSecurity makes the new Feature Key. This Feature Key turns on most of the same features for the standby Firebox X unit as you have on the active Firebox. Here are the exceptions:

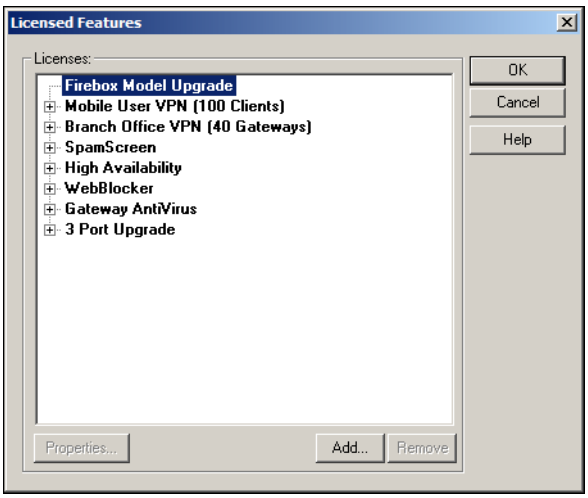
- You must purchase and activate a High Availability license for each Firebox X unit.
- If you apply a model upgrade to one Firebox, then a Firebox model upgrade must be purchased and applied for the standby box, too. For example, if the active Firebox is a Firebox X500 that you upgraded to a Firebox X700, and the partner High Availability Firebox you select is a Firebox X500, you must first upgrade the standby unit to a Firebox X700.

Any other license that is on the active Firebox, such as WebBlocker or SpamScreen or Gateway AntiVirus, is sent to the standby Firebox Feature Key when you activate the High Availability license for the active box.

After you register the High Availability License, get the new Feature Key. You use the same Feature Key for each unit in a High Availability pair. For information about importing a Firebox Feature Key, see the FAQ:

https://www.watchguard.com/support/advancedfaqs/fbx_featurekey.asp

1 From Policy Manager, click **Setup** > **Licensed Features**.
The Licensed Features dialog box appears.



2 Click **Add**.
The Add/Import License Keys dialog box appears.

3 In the **Add/Import License Keys** dialog box, type or paste the Feature Key you get from the LiveSecurity Web site.
You can also click Browse to find a text file with the license keys.

4 Click **OK**.
The High Availability license appears on the Licensed Features dialog box.

Connecting Fireboxes in a High Availability Pair

You must install one of the Fireboxes first. Then you add the Feature Key that turns on High Availability. Then you can configure the second Firebox using the High Availability Wizard or you can configure it manually.

If you do not have a Firebox installed

If you have two new Fireboxes and each Firebox is not installed, you first install one of the two Fireboxes. Use the QuickSetup Wizard to make an initial configuration file and save it to one Firebox. Then import the Feature Key as described above and save the configuration to the Firebox. This turns on the High Availability feature. Continue to the section “Configuring High Availability,” on page 165.

If you have one Firebox installed now.

If you have one Firebox installed but did not start on High Availability for this Firebox, import the Feature Key as described above and save the configuration to the installed Firebox.

Configuring High Availability

There are two methods to configure High Availability. Both methods require that your management station is connected to the standby Firebox with the blue serial cable. Connect one end of the serial cable to the Firebox's Console port. Connect the other end of the serial cable to the management station's COM1 port.

If you do not have the blue serial cable that comes with the Firebox, use a null-modem serial cable.

Your management station computer must also be connected to the same Ethernet network as the Firebox.

1 You can use the Quick Setup Wizard to install High Availability. When you use this method, both Fireboxes must be connected to the network. The High Availability interface must be the trusted interface.

2 You can use the manual method to install High Availability. To use this method it is not necessary that the standby Firebox is connected to the network. Any Firebox interface can be the High Availability interface.

If you use the manual method and the standby Firebox is not connected to the network, connect a crossover Ethernet cable between the management station and the standby Firebox trusted interface.

Note

Each Firebox in a High Availability pair has a different IP address. You must not let a device on the same subnet as the High Availability pair use the Firebox IP addresses. This can cause the traffic between the two devices to stop, and the active Firebox to start a failover to the standby Firebox.

Configuring High Availability with the wizard

Preparation

Before you configure your network for High Availability, make sure that:

- You have the High Availability Feature Keys from the LiveSecurity Web site
- The two Firebox devices are the same model
- The active Firebox is turned on
- The standby Firebox is turned off
- The management station computer is connected to the standby box using the blue serial cable
- The two Firebox devices are connected with Ethernet cables to the network

Each Firebox must use the same method to connect to the network. For example, if the external interface of the first Firebox connects to a hub or switch, then you must connect the external interface of the second Firebox to the same hub or switch. Repeat for each Firebox interface.

The High Availability interface will be the trusted interface.

Configuring using the Wizard

1 Click **Start** > **Programs** > **WatchGuard** > **QuickSetup Wizard**.
The QuickSetup Wizard appears.

2 From the drop-down list, select Click **Establish a High-Availability Firebox Cluster**. Click **Next**.
The High Availability Configuration screen appears.

3 Type the IP address of the active Firebox in the **Active Firebox IP Address** field.
This must be the trusted interface IP address of the active Firebox.

4 In the **Stand-By IP Address** field, type an unused IP address from the same subnet as the High Availability interface on the active Firebox.
The default is the trusted interface.

5 Click **Next**.
The Enter Active Firebox Passwords screen appears.
6 Type the Firebox status passphrase twice.
The status passphrase is the read-only passphrase for the active Firebox.
7 Type the Firebox configuration passphrase twice.
The configuration passphrase is the read-write passphrase for the active Firebox.
8 Click **Next**.
The Copy Active Firebox Setup for Fail-safe Operation screen appears.
9 From the drop-down list, select the Serial Cable method to connect the two Firebox devices. You must also select the computer's serial port from the drop-down list.
10 Type the temporary IP address for the standby Firebox.
You must use an IP address that is different from the management station IP address but is on the same subnet. This IP address can not be the same IP address as the standby Firebox.
11 Click **Next**.
12 When the Wizard tells you, turn on the standby Firebox.
13 The Wizard identifies the Fireboxes and shows you the High Availability Feature Keys. If you have not entered the High Availability Feature Keys, you must do that now.
14 Click **OK**.
15 The Wizard configures both boxes and both boxes start again. The standby box will start in standby mode and the active box will start in active mode.

The configuration is complete.

Configuring High Availability manually

You usually use this method to configure the standby box when the standby box is not connected to the network.

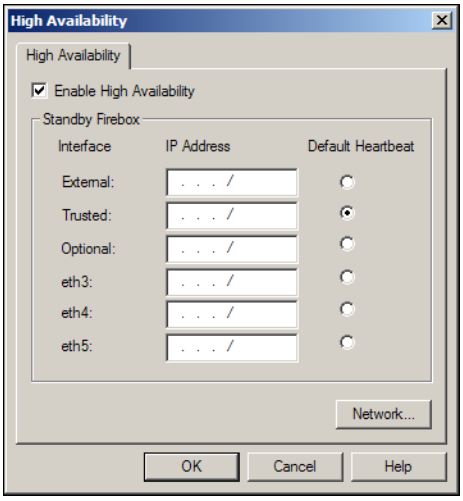
Preparation

Before you manually configure your standby Firebox for High Availability, make sure that:

- The active Firebox has been configured with the High Availability Feature Key. See "Installing High Availability," on page 163
- Your management station computer has the current configuration file for the active Firebox.
- The two Firebox devices are the same model.
- You have the Feature Key that turns on High Availability.
- The standby Firebox is turned off.
- The management station computer is connected to the standby Firebox using the blue serial cable.
- The management station computer is connected to the standby Firebox with an Ethernet cable.
- Configuring manually

1 Open Policy Manager on the management station. Open the configuration that is currently on the active Firebox.
From the Policy Manager, click File > Open Configuration File. Browse to the location of the current configuration of the active Firebox.

2 From Policy Manager, click **Network** > **High Availability**.
The High Availability dialog box appears. You do not see eth3, eth4 and eth5 if you have a Firebox III.



3 Select the **Enable High Availability** checkbox.
The Standby Firebox fields activate.

4 Select the **Default Heartbeat** option for your High Availability interface.
The default is the trusted interface. You can choose a different interface, but you can only use one interface for High Availability.

5 In the **IP Address** field next to the interface you selected, type an IP address from the same subnet as the High Availability interface on the active Firebox. This is the permanent IP address of the standby Firebox.
No other device can use the IP address of the standby Firebox.

6 Click **OK**.

7 Connect the blue serial cable that came with one of the Fireboxes to COM1 of the management station computer and to the Console port of the standby Firebox.

8 From Firebox System Manager, click **Main Menu** > **Tools** > **Advanced** > **Flash Disk Management**.

9 Click the **Boot from the System Area (Factory Default)** option. Click **Continue**.

10 Type an IP address that is in the same subnet as the management station PC but is not the heartbeat IP address. This is the temporary IP address for the Firebox when it is in the factory default mode.

11 Click **OK**.

12 From the drop-down list, select the COM port which connects your management station to the Firebox. Use the blue serial cable.

13 Click **OK**.

14 Turn on the standby Firebox.
The Flash Disk Management tool starts the Firebox and gives it the temporary IP address.

15 Open the Policy Manager with the current configuration for the active Firebox.

16 Click **File** > **Save** > **To Firebox**.

17 Type the temporary IP address that you used in step 10.

18 Type the configuration passphrase. The default passphrase for a new Firebox is wg. Click **OK**.

19 Save the new configuration file to the Firebox. Give the standby Firebox the same configuration passphrase and status passphrase as the active Firebox.
The Policy Manager sends a new flash image to the standby Firebox. The standby Firebox starts again.

If the standby Firebox is connected to the network and the active Firebox is operating, the standby box goes to standby mode. The configuration is complete.

If the standby Firebox is connected only to the management station PC, it goes to active mode. Turn off the standby Firebox. Connect both the standby Firebox and the active Firebox to the network as described at the start of the High Availability Guide. Turn on the active unit if it is not on. Turn on the standby box. The configuration is complete.

Testing the failover process

To make a test of the High Availability configuration, turn off the active Firebox. In less than 15 seconds, the standby Firebox becomes the active Firebox. It gets all packet filter connections that were active before the first Firebox went off line and starts to route traffic for them. Then, turn on the first Firebox. It starts and goes to standby mode.

Indentifying the active and standby Fireboxes.

You can identify which Firebox is the standby Firebox and which Firebox is the active Firebox.

For the Firebox III models:

- The front panel display shows the Armed and SysA lights on the active Firebox.
- The SysA and the SysB lights go on and off on the standby Firebox.

For the Firebox X models:

- The front panel display shows “SysA-Armed” when you push the up button on the active box.
- The front panel display shows “HA-Standby” when you push the up button on the standby box.

Backing up an HA configuration

When a Firebox is operating in a High Availability pair, you can only back up the flash image of the Firebox when it is the active Firebox. This is because the backup image includes the system and policy information, certificates, and licenses that do not exist on the secondary Firebox until failover. To create a backup image (.fbi) of the active Firebox:

1 From Policy Manager, select **File > Save > To Firebox.**

2 Type the configuration passphrase. Click **OK.**

3 Select **Make backup of current flash image before saving**. Type a strong encryption key that is easy to remember.

4 Continue with the operation and make sure the backup is saved to the Backup Image location.

CHAPTER 17

Protecting Users with Gateway AntiVirus for E-mail™

Viruses are malicious computer programs that try to attack your computer or computers on your network. Viruses can be dangerous, and they can cause damage to files and resources. Some viruses find passwords and other sensitive information, and some can use your system or network to attack other systems.

WatchGuard® Gateway AntiVirus for E-mail stops viruses before they get to computers on your network. Gateway AntiVirus for E-mail uses the WatchGuard SMTP Proxy. When you enable Gateway AntiVirus for E-mail, the WatchGuard SMTP Proxy looks at e-mail messages, finds viruses, and removes them.

Note

Gateway AntiVirus for E-mail operates with the SMTP Proxy, for incoming e-mail only. If your organization does not use SMTP to get e-mail, Gateway AntiVirus for E-mail does not give virus protection.

Gateway AntiVirus for E-mail finds viruses encoded with typical e-mail attachment methods. These include base64, binary, 7-bit and 8-bit encoding. Gateway AntiVirus for E-mail does not find viruses in uuencoded or binhex-encoded messages. The type of message is stripped by the Firebox.

About Virus Signatures

When a new virus is identified on the Internet, the features that make the virus unique are identified and recorded. The features that make a virus unique are known as the *virus signature*. Gateway AntiVirus for E-mail uses these virus signatures to find viruses. Gateway AntiVirus for E-mail includes more than 20,000 virus signatures in the default configuration.

New viruses appear on the Internet frequently. To make sure that Gateway AntiVirus for E-mail gives your network the best protection, you must update the virus signatures frequently. You can configure the Firebox® to update virus signatures automatically from WatchGuard. You can also update virus signatures manually on your Firebox. These updates are made available when new viruses are identified.

Note

You must keep virus signatures current to get the best protection from Gateway AntiVirus for E-mail. But, new virus threats appear frequently. WatchGuard cannot guarantee that our product will stop every virus, or prevent damage to your systems or networks from a virus.

Gateway AntiVirus for E-mail Procedures

To use Gateway AntiVirus for E-mail, you must do these steps:

1 Install the Gateway AntiVirus for E-mail feature. See “Installing Gateway AntiVirus for E-mail” on page 170.

2 Enable the Gateway AntiVirus for E-mail feature. See “Enabling Gateway AntiVirus for E-mail” on page 171.

3 Update Gateway AntiVirus for E-mail for the first time. See “Getting Gateway AntiVirus for E-mail Status and Updates” on page 172.

4 Configure Gateway AntiVirus for E-mail system settings. See “Configuring Gateway AntiVirus for E-mail System Settings” on page 173.

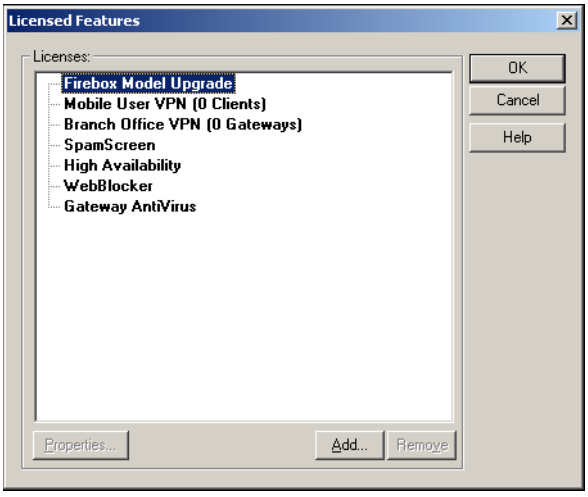
5 Configure Gateway AntiVirus for E-mail in the SMTP Proxy. See “Configuring Gateway AntiVirus for E-mail in the SMTP Proxy” on page 174.

Installing Gateway AntiVirus for E-mail

To install Gateway AntiVirus for E-mail, you must have:

- A Gateway AntiVirus for E-mail license key.
- An SMTP e-mail server behind the Firebox.
- The SMTP Proxy. For information on how to add the SMTP Proxy, see “Configuring Gateway AntiVirus for E-mail in the SMTP Proxy,” on page 174.

1 From Policy Manager, select **Setup** > **Licensed Features**.
The Licensed Features dialog box appears.



2 Click **Add**.

3 In the **Add/Import License Keys** dialog box, type or paste your license key. You can click **Browse** to find it on your computer or network. Click **OK**.
The license key appears on the Licensed Features dialog box.

Note

The Gateway AntiVirus for E-mail product is only available for Firebox X devices. Gateway AntiVirus for E-mail is not supported on Firebox X Edge devices.

Enabling Gateway AntiVirus for E-mail

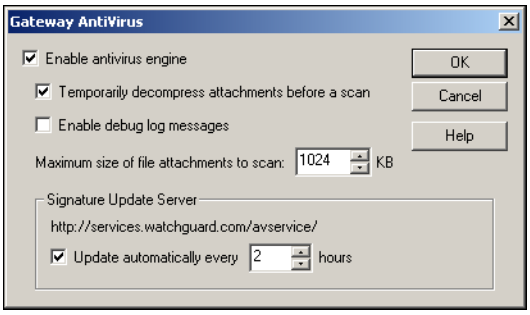
Before you configure and use Gateway AntiVirus for E-mail, you must enable Gateway AntiVirus for E-mail on your Firebox. To do this:

1 Click **Start** > **Programs** > **WatchGuard** > **Firebox System Manager**.

2 In the Connect to Firebox dialog box, type the IP address and status passphrase for the Firebox.

3 Click the Policy Manager button to start Policy Manager. You can select **Tools** > **Policy Manager** from the WatchGuard menu to start Policy Manager.

4 In Policy Manager, select **Setup** > **Gateway AntiVirus**.
The Gateway AntiVirus for E-mail window appears.



5 Select the **Enable antivirus engine** check box. Click **OK**.

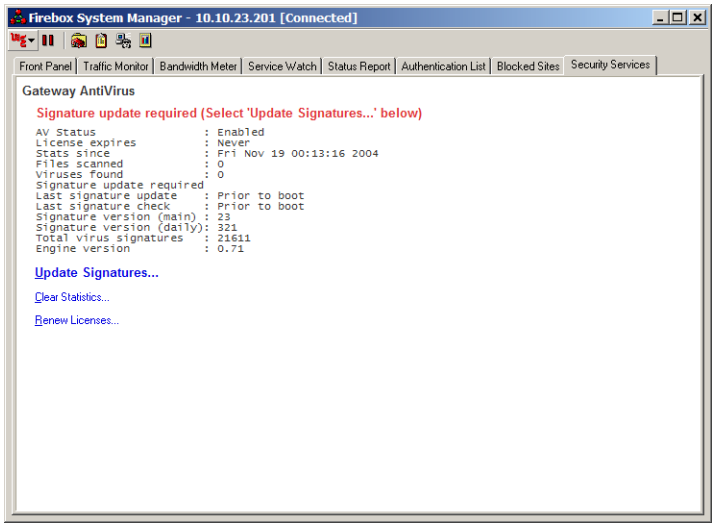
6 Select **File** > **Save** > **To Firebox**.
The first time you enable the antivirus engine, you must save the configuration to the Firebox.

7 Type your configuration passphrase.
The first time you enable the antivirus engine, you must type the read-only passphrase and the configuration passphrase. You must type each password two times.

8 Click **OK**.

Getting Gateway AntiVirus for E-mail Status and Updates

You can see the status and get updates for Gateway AntiVirus for E-mail on the Security Services tab in the Firebox System Manager.



Seeing Gateway AntiVirus for E-mail status

Gateway AntiVirus for E-mail status shows you if Gateway AntiVirus for E-mail protection is enabled. You can also see when the license expires and information about the virus scanner and the virus signatures.

To see Gateway AntiVirus for E-mail status:

1 Start WatchGuard System Manager.

2 Click on the Security Services tab.
Gateway AntiVirus for E-mail status appears. You only see Gateway AntiVirus for E-mail status after you install the Gateway AntiVirus for E-mail license.

Updating Gateway AntiVirus for E-mail signatures

Gateway AntiVirus for E-mail is automatically configured to update the antivirus signatures each two hours. See “Configure Gateway AntiVirus for E-mail” on page 173 to change this setting. You can also update signatures manually. If the virus signatures are not current, you are not protected from the latest viruses.

To update Gateway AntiVirus for E-mail manually:

1 Start WatchGuard System Manager.

2 Click on the Security Services tab.
Gateway AntiVirus for E-mail status appears.

3 Click **Update Signatures**.
The Firebox downloads the latest available signature update for Gateway AntiVirus for E-mail. You can see information about the update in Traffic Monitor.

Updating the antivirus engine

WatchGuard periodically supplies antivirus engine updates for Gateway AntiVirus for E-mail. When an engine update is available, you are notified by a LiveSecurity bulletin e-mail.

It is very important that you update your engine as soon as a new engine is available. Frequently, new signatures only operate with new antivirus engines. You have access to new engines while your Gateway AntiVirus subscription is current.

To download engine updates, log in to your LiveSecurity account at:

https://www.watchguard.com/support

Clear Gateway AntiVirus for E-mail statistics

Clear Gateway AntiVirus for E-mail statistics to see only new statistics.

To clear Gateway AntiVirus for E-mail statistics:

1 Start WatchGuard System Manager.

2 Click on the Security Services tab.
Gateway AntiVirus for E-mail status appears.

3 Click **Clear Statistics**.

4 You are prompted for the configuration passphrase. Type the configuration passphrase and click **OK**.

The statistics are cleared and the Firebox starts to record statistics again. The **Stats since** field shows the last time and date that the statistics were cleared. The **Files scanned** and **Viruses found** fields show zeroes until a new file is examined or a virus is found.

Note

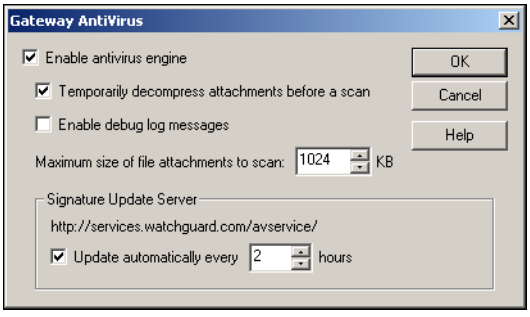
After you clear statistics, you can still see older log messages in the log files.

Configuring Gateway AntiVirus for E-mail System Settings

You use the Gateway AntiVirus for E-mail™ window to enable Gateway AntiVirus for E-mail and configure Gateway AntiVirus for E-mail. This window configures the Gateway AntiVirus for E-mail feature for all SMTP Proxies on the Firebox. You can also create different configurations in each SMTP Proxy. For more information, see "Configuring Gateway AntiVirus for E-mail in the SMTP Proxy," on page 174.

Configure Gateway AntiVirus for E-mail

1 In Policy Manager, select **Setup** > **Gateway AntiVirus**. The **Gateway AntiVirus** dialog box appears.



2 If Gateway AntiVirus for E-mail is not enabled, select the **Enable antivirus engine** check box.

3 To temporarily decompress files that are compressed to examine contents for viruses, select the **Temporarily decompress attachments before a scan** check box.
This option allows the Firebox to examine the contents of compressed files, for example Zip files, TAR files, and TGZ files.

Note

Gateway AntiVirus for E-mail can only examine one level of a compressed file. Hackers can hide viruses in compressed files that are inside other compressed files. Gateway Antivirus for E-mail supports several compression methods. See the Release Notes for this product for a list of the compression file types supported by this release.

4 To record debug log messages for Gateway AntiVirus for E-mail, select the **Enable debug log messages** check box.
Use this check box to record log messages about the actions of the antivirus service. It is not usually necessary to record these messages unless the antivirus service does not operate correctly. If this option is selected, log messages are recorded that give more detail about the operation of the antivirus engine. These messages can be used with Technical Support to troubleshoot problems.

5 You can set a maximum attachment size to examine in the **Maximum size of file attachments to scan** field.
Gateway AntiVirus allows you to configure the attachment file size from 128 KB to 4096 KB. You can use the arrows to move up or down in 128 KB increments, or type a number between 10 and 4096.

Note

Note that this setting does not automatically change the setting in the SMTP Proxy general tab for Maximum Size. The smallest size setting of these two properties takes precedence.

6 To get signature updates automatically, select the **Update automatically** check box. Select or type the number of hours between update checks.
Signature updates allow Gateway AntiVirus for E-mail to protect your system from new virus threats that appear. Set the Firebox to get frequent automatic updates to protect your network better.

Configuring Gateway AntiVirus for E-mail in the SMTP Proxy

You use Gateway AntiVirus for E-mail™ to find and stop viruses with the SMTP Proxy. The Firebox uses the SMTP Proxy to examine e-mail messages.

This guide gives you the basic procedure to add an SMTP Proxy, and the procedure for configuring Gateway AntiVirus for E-mail. For full configuration information for the SMTP Proxy, see "Configuring an SMTP Proxy Service" on page 70.

Add an SMTP Proxy with Gateway AntiVirus for E-mail

To add an SMTP Proxy and configure Gateway AntiVirus for E-mail:

1 Start Policy Manager.

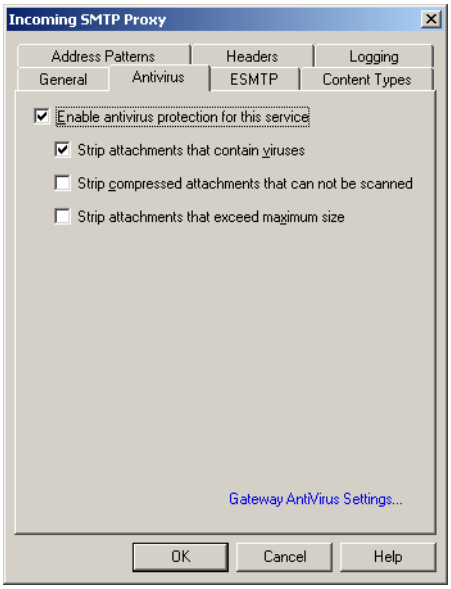
2 Select **Edit** > **Add Service**, expand the **Proxies** folder, and select **SMTP**.

3 Click **Add**.

4 Type a name for the service and click **OK**.

5 Configure the Incoming and Outgoing connections and traffic configurations for your network.

6 Click the **Properties** tab. Click the **Incoming** button. Click the **AntiVirus** tab.
The AntiVirus configuration for this Proxy appears.



7 To enable AntiVirus on this Proxy, select the **Enable antivirus protection for this service** check box.

8 To remove attachments that contain viruses, select the **Strip attachments that contain viruses** check box.

Note

This option is enabled in the default configuration. It is recommended that you use this option. Your users are only protected from viruses if this check box is selected.

9 To remove compressed attachments that can not be scanned by Gateway AntiVirus for E-mail, select the **Strip compressed attachments that can not be scanned** check box.
Compressed attachments that can not be scanned include files that use unsupported compression formats such as RAR 3.0, and password-protected ZIP or other compressed files. This is not enabled by default. It is not recommended that you enable this option.

10 To remove attachments that exceed the maximum size, select the **Strip attachments that exceed maximum size** check box.
You can configure the maximum size in the Gateway AntiVirus for E-mail dialog box. See "Configuring Gateway AntiVirus for E-mail System Settings" on page 173. This setting is not enabled by default, and it is not recommended that you enable it.

11 Click **OK**.
The Service Properties window appears.

12 When you complete the configuration for the SMTP Proxy, click **OK**.

13 Click **OK** to close the **Add Service** dialog box.

14 Save the configuration to the Firebox. Select **File** > **Save** > **To Firebox**.

15 Select a configuration file to save, or type the name of a new file, and click **Save**.

16 Type the configuration passphrase in the **Save to Firebox** dialog box.

17 Click **Continue** to save the file to the Firebox.

18 Click **OK** after the Firebox is configured.

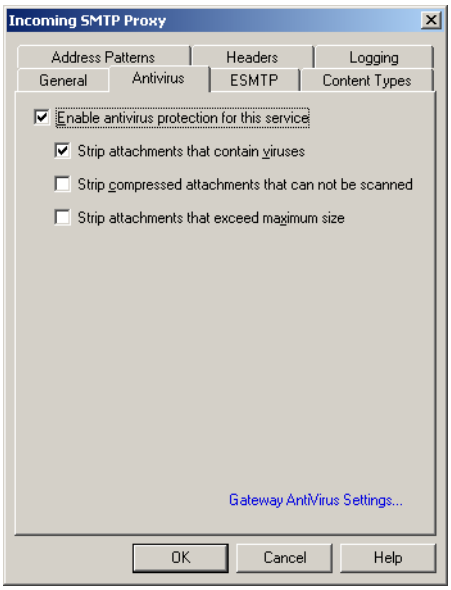
Configure Gateway AntiVirus for E-mail for an existing SMTP Proxy

To add Gateway AntiVirus for E-mail to an existing SMTP Proxy:

1 Start Policy Manager.

2 Double-click the SMTP Proxy service.

3 Click the **Properties** tab. Click the **Incoming** button. Click the **AntiVirus** tab.
The AntiVirus configuration for this Proxy appears.



4 To enable AntiVirus on this Proxy, select the **Enable antivirus protection for this service** check box.

5 To remove attachments that contain viruses, select the **Strip attachments that contain viruses** check box.

Note

This option is enabled in the default configuration. It is recommended that you use this option. Your users are only protected from viruses if this check box is selected.

6 To remove compressed attachments that can not be scanned by Gateway AntiVirus for E-mail, select the **Strip compressed attachments that can not be scanned** check box.
Compressed attachments that can not be scanned include files that use unsupported compression formats such as RAR 3.0, and password-protected ZIP or other compressed files. This is not enabled by default. It is not recommended that you enable this option.

7 To remove attachments that exceed the maximum size, select the **Strip attachments that exceed maximum size** check box.
You can configure the maximum size in the Gateway AntiVirus for E-mail dialog box. See "Configuring Gateway AntiVirus for E-mail System Settings" on page 173. This setting is not enabled by default, and it is not recommended that you enable it.

8 Click **OK**.
The Service Properties window appears.

9 When you complete the configuration for the SMTP Proxy, click **OK**.

10 Save the configuration to the Firebox. Select **File** > **Save** > **To Firebox**.

11 Select a configuration file to save, or type the name of a new file, and click **Save**.

12 Type the configuration passphrase in the **Save to Firebox** dialog box.

13 Click **Continue** to save the file to the Firebox.

14 Click **OK** after the Firebox is configured.

Using Gateway AntiVirus for E-mail with More Than One Proxy

You can use more than one SMTP Proxy to find and remove viruses for different servers in your organization.

Each proxy that uses Gateway AntiVirus for E-mail is configured with options that are unique to that proxy. For example, you can use different proxy antivirus configurations for e-mail that is for different servers or different destinations.

Gateway AntiVirus for E-mail Headers

Gateway AntiVirus for E-mail adds a header to each incoming e-mail message. An e-mail message can include multiple parts separated by MIME boundaries (multipart MIME). Each MIME part has a separate set of headers. If a part includes an attachment, Gateway Antivirus for E-mail adds the header **X-AntiVirus** to the set of headers. This header shows antivirus activity for the part. The X-AntiVirus header shows if the message is clean, infected with a virus, or if there is a different error in the antivirus procedure. If a part includes an attachment, the antivirus action is included in the header. The action can be **allow** or **deny**.

In this example, an attachment is infected with a virus, and the virus is detected by Gateway AntiVirus for E-mail:

`X-AntiVirus: attachment_name is infected with virus virus_name; action=deny`

If an attachment is denied, the body for that part of the message is replaced. The new part is a message similar to the value of the X-AntiVirus header, for example:

`Attachment attachment_name is infected with virus virus_name, denying attachment`

Monitoring Gateway AntiVirus for E-mail Activity

You can monitor Gateway AntiVirus for E-mail with the logging tools. The WatchGuard System Manager includes reports and real-time log message monitors.

When Gateway AntiVirus for E-mail examines an attachment or identifies a virus and removes an attachment, it records a log message in the log file.

These are example Gateway AntiVirus for E-mail log messages in the Simple Log format:

Message	Meaning
AV: attachment *filename* is clean Where *filename* is the name of the file that is scanned	The Firebox examined an attachment that does not contain a virus.
AV: attachment *filename* is infected with virus *virusname*, denying attachment Where *filename* is the file that is scanned, and *virusname* is the name of the virus that is detected.	The Firebox examined an attachment and found a virus. The attachment was removed.
AV: attachment *size* not scanned due to size, denying attachment Where *size* is the size of the file that is not scanned.	Gateway AntiVirus for E-mail found a file that exceeds the size limit, and removed it. This occurs when Gateway AntiVirus for E-mail is configured to strip attachments that exceed the maximum size.

The example below shows a diagnostic log. In addition to the messages listed above, it includes log messages that describe the operation of each Gateway AntiVirus for E-mail action.

```
12/03/04 11:09  smtp-proxy[197]:  Entering InitAV
12/03/04 11:09  smtp-proxy[197]:  [60.100.253.9:4847 10.9.9.3:25] removing ESMTP keyword "PIPELINING"
12/03/04 11:09  smtp-proxy[197]:  [60.100.253.9:4847 10.9.9.3:25] removing ESMTP keyword "VRFY"
12/03/04 11:09  smtp-proxy[197]:  [60.100.253.9:4847 10.9.9.3:25] removing ESMTP keyword "ETRN"
12/03/04 11:09  smtp-proxy[197]:  [60.100.253.9:4847 10.9.9.3:25] removing ESMTP keyword "XVERP"
12/03/04 11:09  smtp-proxy[197]:  AV: attachment avnormal.txt will be scanned
12/03/04 11:09  avd[138]:  Accepted client on 10
12/03/04 11:09  smtp-proxy[197]:  AV: received response, response is /tmp/clamav/s0 4096
12/03/04 11:09  smtp-proxy[197]:  AV: socket setup complete
12/03/04 11:09  smtp-proxy[197]:  AV: entering AVCleanSpace
12/03/04 11:09  smtp-proxy[197]:  AV: scan file path /tmp/clamav/s0/1197, av state 0, max file size 4194304
12/03/04 11:09  smtp-proxy[197]:  AV: attachment encoding is base64
12/03/04 11:09  smtp-proxy[197]:  AV: write to disk complete, bytes written 33537
12/03/04 11:09  smtp-proxy[197]:  AV: scan command is "scan default 197 /tmp/clamav/s0/1197"
12/03/04 11:09  smtp-proxy[197]:  AV: scan response is "clean 197"
12/03/04 11:09  smtp-proxy[197]:  AV: attachment avnormal.txt is clean
12/03/04 11:09  smtp-proxy[197]:      mail from address <user@watchguard.com>
12/03/04 11:09  smtp-proxy[197]:      rcpt to address <user2@watchguard.com>
12/03/04 11:09  smtp-proxy[197]:  AV: base64 encode attachment
12/03/04 11:09  smtp-proxy[197]:  AV: attachment read from disk (33537) and written to socket (46071)
12/03/04 11:09  smtp-proxy[197]:  AV: antivirus scan done
12/03/04 11:09  smtp-proxy[197]:  AV: entering AVCleanSpace
12/03/04 11:09  smtp-proxy[197]:  AV: attachment avviral.txt will be scanned
12/03/04 11:09  smtp-proxy[197]:  AV: scan file path /tmp/clamav/s0/2197, av state 0, max file size 4194304
12/03/04 11:09  smtp-proxy[197]:  AV: attachment encoding is base64
12/03/04 11:09  smtp-proxy[197]:  AV: write to disk complete, bytes written 68
12/03/04 11:09  smtp-proxy[197]:  AV: scan command is "scan default 197 /tmp/clamav/s0/2197"
12/03/04 11:09  smtp-proxy[197]:  AV: scan response is "virus 197 Eicar-Test-Signature"
12/03/04 11:09  smtp-proxy[197]:  AV: antivirus action is deny
12/03/04 11:09  smtp-proxy[197]:  AV: attachment avviral.txt is infected with virus Eicar-Test-Signature,
denying attachment
12/03/04 11:09  smtp-proxy[197]:      mail from address <user@watchguard.com>
12/03/04 11:09  smtp-proxy[197]:      rcpt to address <user2@watchguard.com>
12/03/04 11:09  smtp-proxy[197]:  AV: antivirus scan done
12/03/04 11:09  smtp-proxy[197]:  AV: entering AVCleanSpace
```

CHAPTER 18

SpamScreen

Unwanted e-mail, also known as spam, fills the average inbox at an astonishing rate. Some experts predict that the total number of spam e-mail messages sent each day will increase from 10 billion in 2003 to 30 billion by 2006. This large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources.

The WatchGuard® SpamScreen™ option increases your capacity to catch spam at the edge of your network when it tries to come into your system. You can use the SMTP Proxy of your WatchGuard firewall to strip or tag incoming spam. With SpamScreen enabled, the WatchGuard SMTP Proxy examines the header content of each message and decides if the message is spam.

Note

In this User Guide, the word Firebox refers to a Firebox® III or a Firebox® X hardware device unless we tell you differently.

SpamScreen Options

You can configure SpamScreen™ to customize how the Firebox® identifies e-mail as spam and blocks, tags, or allows the messages it identifies as spam.

SpamScreen has two methods to identify an e-mail message as spam. With the first method, SpamScreen uses the IP address of the sender of the e-mail. It makes sure that the sender is not on one or more RealTime Blackhole List (RBL) servers. If the sender is on an RBL server, then the Firebox identifies the message as spam. An RBL server is a server which keeps the IP addresses of known sources of spam. It also keeps the IP addresses of computers that might be vulnerable to spam attacks. For example, mail relays are frequently vulnerable to a spam attack. SpamScreen also makes sure that the domain name of the source is correct. An RBL server can not be used as a standard DNS server.

The second method SpamScreen uses to identify spam is to apply a list of rules to e-mail message headers. Each rule has a positive or negative weight. The sum of the weight values of rule matches are recorded for each message. If the sum is more than a limit you set, the Firebox identifies the message as spam. For more information, see "Configuring Spam Rules" on page 186.

You can also configure what the Firebox does with a message after it identifies it as spam. The SMTP Proxy can allow the message, deny it, or tag it as spam before it sends it to the recipient.

For more information on features of SpamScreen, see the online support resources at:
https://www.watchguard.com/archive/showhtml.asp?pack=5985

Customizing SpamScreen using Multiple Proxies

If you have multiple SMTP servers, you can configure more than one SMTP Proxy service to use SpamScreen™. This lets you create custom rules for different groups in an organization. For example, you can use the RBL server method to identify spam for your IT department while at the same time you allow all e-mail to your management and use a spam tag for the marketing team.

When you make more than one SMTP Proxy service, the Rules Lists and RBL Lists apply to all of the services. You can not use different lists for different SMTP Proxy services.

For more information on using more than one SMTP Proxy service with SpamScreen, see the FAQ at:
www.watchguard.com/support/advancedfaqs/spam_multproxies.asp

Installing SpamScreen

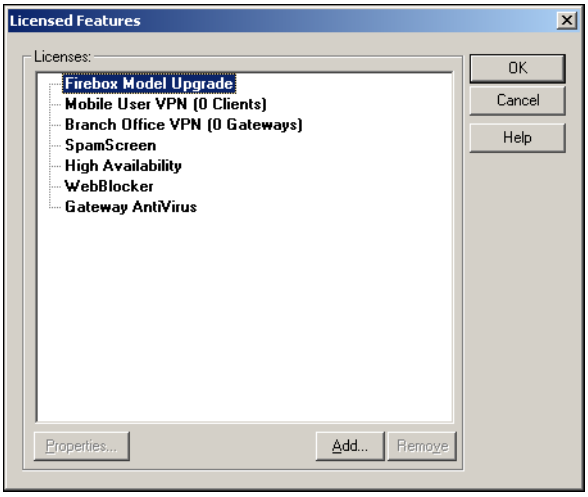
Before you install SpamScreen™, you must have:

- A SpamScreen license key certificate
- An e-mail server behind the Firebox®
- A SMTP Proxy service

For information on the SMTP Proxy service, see the *WatchGuard System Manager User Guide*.

To install SpamScreen:

1 From Policy Manager, select **Setup** > **Licensed Features**.
The Licensed Features dialog box appears.



2 Click **Add**.

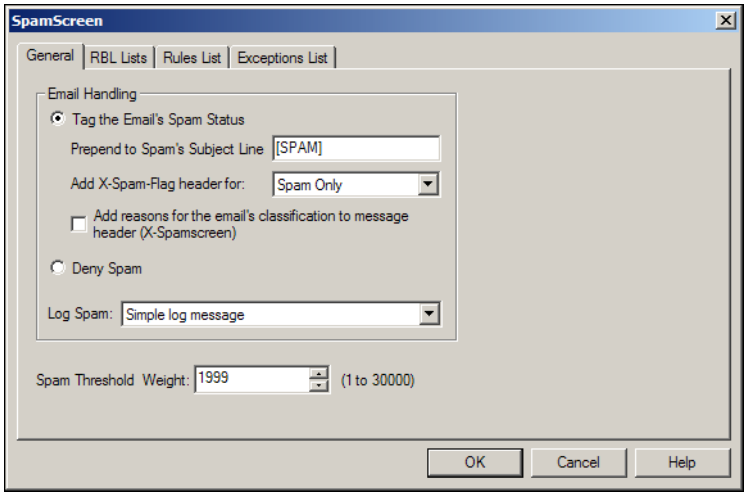
3 In the **Add/Import License Keys** dialog box, type or paste your license key. You can also click **Browse** to find a text file with the license key values. Click **OK**.
The new license appears in the Licensed Features dialog box.

Starting SpamScreen

From the WatchGuard Policy Manager, select **Setup** > **SpamScreen**. The SpamScreen™ dialog box appears. You use this dialog box to configure:

- The method the Firebox uses to identify spam; and
- The action the Firebox takes after it identifies a message as spam.

You also use the SpamScreen dialog box to configure the RBL server IP addresses, spam rules, log message type, and exceptions to spam rules.



Configuring How the Firebox Handles Spam

The Firebox® uses SpamScreen™ rules to handle e-mail messages. It can:

- **Deny** — Block the spam message without a reply.
- **Tag** — Identify the message as spam or not spam and allow spam messages to go to the recipient.
- **Allow** — Deliver spam messages without a tag.

We recommend that initially you do not use the Deny option. Use the Tag option and monitor the results for a period of time before you enable the Deny option.

About SpamScreen headers and tags

The Firebox can add SpamScreen messages to message headers and to the e-mail subject. You use the SpamScreen dialog box to configure the tag feature to do this.

X-SpamScreen header

The Firebox adds an X-Spamscreen header to each e-mail message it examines. This is an example:

```
X-Spamscreen: Protected by WatchGuard (WGTI) SpamScreen (TM)
v7.3.B1823 Copyright (C) 1996-2004 WGTI
```

You can also configure SpamScreen to show a description of the method the Firebox used to examine the e-mail message. In this example, the X-Spamscreen header has more information including: the

message spam score and the spam limit you set. For more information on weight, see "Configuring Spam Rules" on page 186.

```
X-Spamscreen: Protected by WatchGuard (WGTI) SpamScreen (TM)
  v7.3.B1823 Copyright (C) 1996-2004 WGTI
  Results of SpamScreen: 2000  From contains advertising fingerprint
  Score   : 2000
  Required: 1999
```

X-Spam-Flag header

The Firebox can tag each message it examines with an "X-Spam-Flag" header. This header gives more information about the e-mail message. If the value of X-Spam-Flag is "YES", then the Firebox identifies the message as spam. If the value of the X-Spam-Flag is "NO", the Firebox does not identify the message as spam. You can use this header to sort spam e-mail into different folders than regular e-mail.

This example shows a message header with the X-Spamscreen and X-Spam-Flag information with the Firebox configured to tag all e-mail and to include SpamScreen information.

```
X-Spam-Flag: NO
X-Spamscreen: Protected by WatchGuard (WGTI) SpamScreen (TM)
        v7.3.B1825 Copyright (C) 1996-2004 WGTI
        Results of spamscreen:
            701    Subject contains "FREE" in CAPS
        Score   : 701
        Required: 1999
```

Spam subject line

You can configure SpamScreen to add text to the subject of e-mail messages the Firebox identifies as spam. You can also customize the text that appears. This example uses the text [SPAM]:

```
Subject: [SPAM] Free auto insurance quote
```

Example message header

Note that the X-Spam-Flag header appears because SpamScreen has been configured to tag e-mail messages. SpamScreen has also been configured to include processing information in the X-Spam-Screen header and to prepend the subject line with a specific string, in this case [SPAM]:

A full e-mail message header includes information about the source, the destination, and the route of the message. When the Firebox adds the SpamScreen information, a typical e-mail message appears like the following example. For this message, the Firebox is configured to add the X-Spam-Flag and X-Spamscreen headers and to add [SPAM] to the subject.

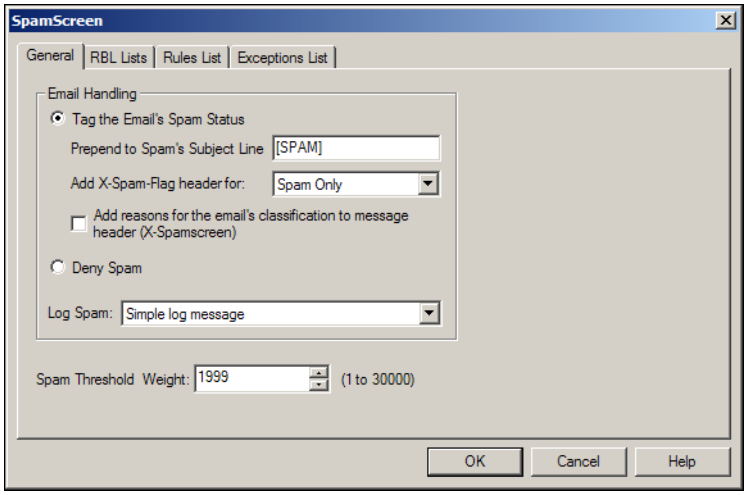
```
Return-Path: <johndoe@sparta.iceberg2.watchguard.com>
Delivered-To: johndoe@thebes.iceberg.watchguard.com
Received: from iceberg.watchguard.com (unknown [60.100.253.9])
        by thebes.iceberg.watchguard.com (Postfix) with ESMTP id E7B0918C1F
        for <johndoe@thebes.iceberg.watchguard.com>; Wed,  2 Jul 2003 08:33:07 -0700 (PDT)
MIME-Version: 1.0
Message-Id: <9402060055.AA06427@iceberg.watchguard.com>
To: johndoe@thebes.iceberg.watchguard.com
From: dude@berrypatch.com
Subject: [SPAM] You've got mail and you've been approved!
X-Spam-Flag: YES
X-Spamscreen: Protected by WatchGuard (WGTI) SpamScreen (TM)
        v7.0.B1346 Copyright (C) 1996-2003 WGTI
        Results of spamscreen:
            2630    Subject talks about being approved
        Score   : 2630
        Required: 1999
        Date: Wed,  2 Jul 2003 15:33:08 +0000 (UTC)
Today is your lucky day! you've been approved to get a free e-mail account from our deluxe service.
```

For information on how to view full message headers, see “Viewing message header notifications” on page 190.

Tagging messages

To *tag* an e-mail message is to examine the contents and identify the message as unwanted or valuable. Unwanted e-mail is known as *spam*. Valuable e-mail is frequently known as *ham*. When you configure SpamScreen to tag e-mail, the Firebox identifies spam messages and then sends them to the recipient.

1 From Policy Manager, select **Setup** > **SpamScreen**.
The SpamScreen dialog box appears.



2 To add the X-Spam-Flag header to each e-mail message, select **Tag the e-mail's Spam Status** checkbox.

3 To add text to the subject of each spam message, type the word in the **Prepend to Spam's Subject Line** field.
The default value is [SPAM].

4 Use the **Add X-Spam-Flag header for** drop-down list to select if the Firebox adds the X-Spam-Flag header to all e-mail messages or only to spam messages.

5 To include a description of the method used to examine the message in the X-Spamscreen header, select the **Add reasons for the e-mail's classification to message header (X-Spamscreen)** checkbox.

6 Click **OK**.

Denying spam

The Firebox can block all messages it identifies as spam. This is a good method to prevent spam, but it also adds risk that the Firebox will block an important message that is not spam. We recommend that you initially use the tag option. Only use the Deny option if you find the tag option correctly identifies the spam and ham for your users.

1 From Policy Manager, select **Setup** > **SpamScreen**.

2 On the General tab, select the **Deny Spam** option.

Allowing spam

To allow all e-mail messages, including spam, leave both options on the SMTP proxy disabled, as described in the next section "Determining how SpamScreen Identifies Spam." SpamScreen allows spam e-mail messages and tags them with only the default X-SpamScreen header, as described in "X-SpamScreen header" on page 181.

Logging spam

You can configure the Firebox to record a log message when it identifies an e-mail as spam. There are three **Log Spam** options:

- **No log message** — The Firebox does not record a log message when it identifies an e-mail as spam.
- **Simple log message** — The Firebox records one log message with the sender and recipient.
- **Verbose log message** — The Firebox records the contents of the X-Spamscreen header in the log file.

Determining How SpamScreen Identifies Spam

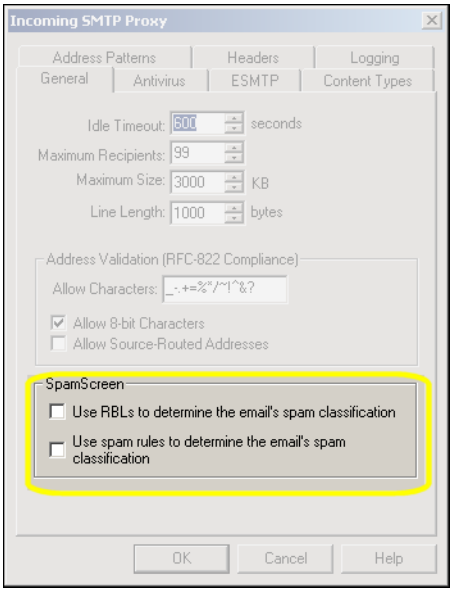
SpamScreen™ includes two methods to identify spam message. The first method makes sure that the IP address of the sender is not on a list of known sources of spam. There are many open source and subscription servers which keep such lists. The Realtime Blackhole List (RBL) servers are one example. The Firebox can also use an MX record lookup to make sure that the e-mail server is at the location of the sender.

The second method that SpamScreen uses to identify a spam message is to examine the message against a group of rules. Spam messages frequently have the same components, such as the sender name or a "bulk mail" header. For more information on rules, see "Configuring Spam Rules" on page 186.

1 From the Policy Manager, double-click the **SMTP Proxy** icon.
The SMTP Proxy Properties dialog box opens.

2 Click the **Properties** tab.

3 Click **Incoming**.
The Incoming SMTP Proxy dialog box appears displaying the General tab.



4 To use the RBL servers, select the **Use RBLs to determine the e-mail's spam classification** checkbox.
For information on how to configure the RBL server IP addresses, see "Configuring RBL/DNS Servers," on page 185.

5 To use rules that identify known spam characteristics, select the **Use spam rules to determine the e-mail's spam classification**.
For more information on how to configure spam rules, see "Configuring Spam Rules" on page 186.

6 If it is necessary to temporarily disable the SpamScreen feature, clear the RBL and spam rules checkboxes. The Firebox allows all e-mail messages.

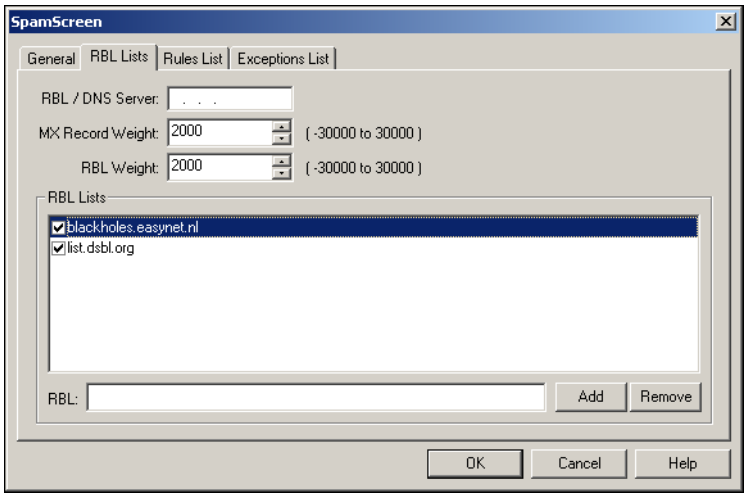
Configuring RBL/DNS Servers

A RealTime BlackHole List (RBL) is a name server that keeps IP addresses that are thought to be the source of spam, a spam relay, or Internet Service Providers that allow or support spam. If the message comes from an address on an RBL, the Firebox identifies the message as spam.

To be a host for an RBL server can be a risk. The network host is frequently the recipient of a legal action. As a result, the list of available RBLs changes for each SpamScreen™ software version. Also because of this, some RBL providers charge a subscription fee. We recommend that you do regular maintenance on the list of RBL servers which your Firebox uses. You can find more information on Web sites which have information about the risks and inappropriate use of e-mail.

Use this procedure to specify the RBL values used by SpamScreen:

1 From the Policy Manager, select **Setup** > **SpamScreen**. Click the **RBL Lists** tab.



2 In the **RBL/DNS Server** field, type the IP address of the server.
This is frequently the IP address of your DNS server. It can also be the DNS server of your Internet Service Provider. The Firebox uses this server to do an MX record lookup on the sender of each e-mail message.

3 When the Firebox does an MX record lookup and can not confirm that the domain name of the sender is real, it adds the **MX Record Weight** to the total Spam Weight. While the default value of 2000 is sufficient in most conditions, you can change this value.

4 When the Firebox confirms that the sender IP address matches an address on one or more RBL lists, it adds the **RBL Weight** to the total Spam Weight. While the default value of 2000 is sufficient in most conditions, you can change this value.

Adding RBL Servers

A list of RBL servers appears on the **RBL Lists** tab. To enable an RBL server on the list, select its checkbox. You can also use the **Add** and **Remove buttons** to add or remove other RBL servers.

You can find more RBL servers at these Web sites:

- http://www.mail-abuse.org
- http://www.abuse.net

Configuring Spam Rules

You can configure SpamScreen™ to use rules about mail header information to identify spam. The Firebox examines the e-mail message and finds the probability that an e-mail message is spam. Each rule has a weight. The Firebox adds all the matching rules together and gives the message a score. If the total Spam Weight is larger than a limit you set, the Firebox identifies the message as spam.

The Firebox only examines the e-mail message header. It does not examine the content of the message. A message header is the component of an e-mail that includes: subject, date, sender, recipient. Each header has a title followed by a ":" and then a value. For example, you can find the date a message is sent in the "Date:" header. A message header appears at the top of a message. SpamScreen rules are written in the language "regular expression" and examine e-mail headers to find pattern matches.

WatchGuard customers frequently make SpamScreen rules to help them find and tag spam. An example of a rule is to examine the e-mail header for the text string "free". If the message has a header with the word "free", the total Spam Weight increases. You can also make rules about incorrect dates, empty fields, or MIME types.

You assign a weight to each rule. If a message matches more than one rule, it is more likely the Firebox will identify it as spam. You can also assign a negative weight to a rule. This helps the Firebox to not identify good e-mail as spam.

For example, you can set up rules with positive weights for messages with the word "sale." At the same time, you can set up rules with negative weights for e-mail sent by vendors you regularly do business with. An e-mail from your vendor about "SALE!" in the subject matches two rules: a positive weight for the word "sale" and a negative weight for the sender. When the Firebox adds the two weights, it does not identify the message as spam.

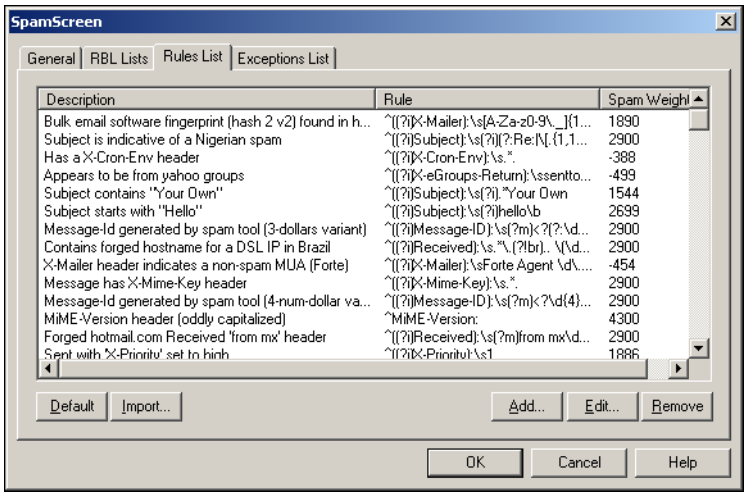
Note

Rules apply only to e-mail headers and not to e-mail content. SpamScreen does not examine the text of e-mail messages.

The default SpamScreen configuration includes many rules which are sufficient for most installations. If you are an advanced user, you can add new rules or remove or change the default rules.

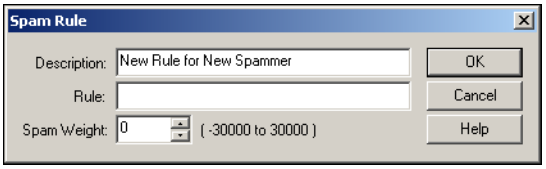
Adding spam rules

1 From the Policy Manager, select **Setup** > **SpamScreen**. Click the **Rules List** tab.



2 To remove a rule, highlight the rule in the **Rules List**. Click **Remove**.

3 To add a new rule, click **Add**.
The Spam Rule dialog box appears.



4 In the **Description** text box, type a description for the rule. This text appears in the Rules List and helps you find a rule.
An example is "Subject starts with "Sale"."

5 In the **Rule** text box, type the spam rule. Rules use Perl compatible regular expression syntax. For more information on Perl compatible regular expressions, browse to:
http://www.pcre.org/pcre.txt

6 Type a weight for the rule in the **Spam Weight** field. You can type a value from -30,000 to 30,000. Positive numbers are for rules that identify spam. Negative numbers are for rules that identify ham.

Restoring default rules

To restore the default configuration for spam rules, on the **Rules List** tab, click the **Default** button.

Importing rules

You can import rules from a file. This can save you time. The rules must be in the same format as the configuration file. The syntax is:

weight “description” rule

Examples:
1886 "Sent with 'X-Priority' set to high" ^((?i)X-Priority):\s+1
1594 "Message has X-Library header" ^((?i)X-Library):\s+.*.
-388 "Has a X-Cron-Env header" ^((?i)X-Cron-Env):\s+.*.
4300 "Message has X-x header" ^((?i)X-x):\s+.*.
-192 "Has a Resent-To header" ^((?i)Resent-To):\s+.*.

1 From the Rules List tab of the SpamScreen dialog box in Policy Manager, click **Import**.

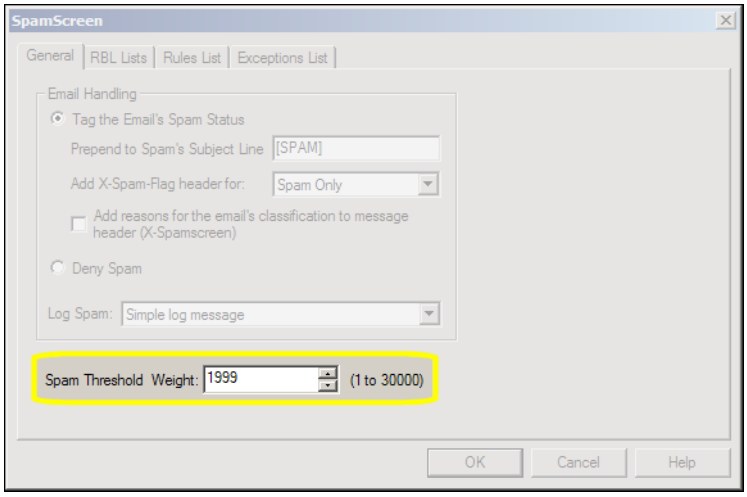
2 Browse to locate the file. Select the file, and click **Open**.

For more information on SpamScreen rules, see the LiveSecurity archive at:
www.watchguard.com/archive/showhtml.asp?pack=7131
www.watchguard.com/archive/showhtml.asp?pack=7372

Defining spam threshold weight

E-mail must be more than a Spam Weight limit that you set before the Firebox can identify it as spam. To change the **Spam Threshold Weight** value, open the SpamScreen dialog box.

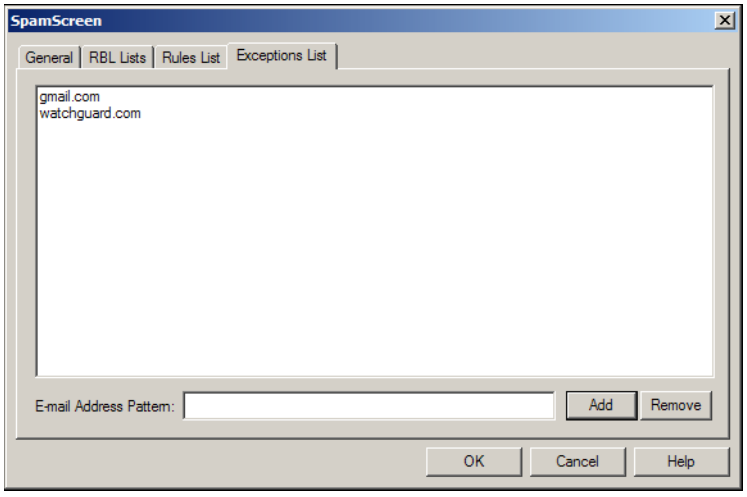
When you increase the Spam Threshold Weight, you make it harder for the Firebox to identify a message as spam. When you decrease the Spam Threshold Weight, you make it easier for the Firebox to identify a message as spam.



Configuring Exceptions to the Spam List

At times, the Firebox identifies a message as spam when it is not spam. If you know the address of the sender, you can configure the Firebox with an exception after which it does not examine the messages from that source.

1 From the Policy Manager, select **Setup** > **SpamScreen**. Click the **Exceptions** tab.



2 In the **E-mail Address Pattern** text box, type the domain name or e-mail address of the sender. Click **Add**.

The host name or e-mail address appears in the Exceptions to Spam list. SpamScreen does not examine messages from that address.

Blocking addresses not on the spam list

If you are attacked by a spam source that is not on an RBL list, you can use the SMTP Proxy to block all messages from that source.

Note

When you use the SMTP Proxy to block an address pattern, you prevent all e-mail from that source. Use caution when using this feature.

1 From the Policy Manager, double-click the **SMTP Proxy** icon.
The Properties dialog box opens.
2 Click the **Properties** tab.
3 Click **Incoming**.
The Incoming SMTP Proxy dialog box appears displaying the General tab.
4 Click the **Address Patterns** tab.
5 Use the **Category** drop-down list to select **Denied From**.
6 Type the address pattern in the text box to the left of the **Add** button.
7 Click **Add**.
The address pattern appears in the pattern list. Repeat for the address pattern of each spammer not blocked automatically by SpamScreen.
8 Click **OK**.

For more information about using the SMTP proxy to block an address pattern, see the FAQ:
www.watchguard.com/support/AdvancedFaqs/proxy_smtp.asp

Monitoring SpamScreen Activity

You can use a number of methods to monitor SpamScreen™. The WatchGuard System Manager includes reports and real-time log message monitors. You can also use your e-mail software.

Viewing message header notifications

Most e-mail systems use special instructions to show full message headers. The instructions that follow are the procedures for the most frequently used e-mail systems. Use your e-mail system documentation if your software is not in this list.

Microsoft Outlook 97 and Microsoft Outlook Express

1 Open the message.
2 Select **File** > **Properties**.
3 Click the **Details** tab.

Microsoft Outlook 98 and later

1 Open the message.
2 Select **View** > **Options**.
The Internet headers field displays the entire message header.

Netscape Messenger

1 Open the message.

2 Select **View** > **Headers** > **All.**

Interpreting log messages

When SpamScreen identifies a message as spam, it records a log message in the log file. Usually, these log messages give a cause for the identification as spam.

These are example SpamScreen log messages in the Simple Log format:

Message	Description
Found spam from server-IP (reason) from user@domain Where *server-ip* is the IP address of the sending SMTP server, *reason* explains why SpamScreen marked the message as spam and *user@domain* is the sender of the message.	The Firebox identified the message as spam based on the SpamScreen rules.
user@domain overrides spam list Where *user@domain* is the sender of the message	The sender address was found on the Exceptions list. The Firebox did not examine the message.

The example below is of a Verbose Log. In addition to the fields on the previous table, it lists the rules hit, the total score, and the threshold.

```
05/31/03 16:06  smtp-proxy[143]: (spamscreen) e-mail received from <od@yahoo.com>, marked as spam
05/31/03 16:06  smtp-proxy[143]:     Results of spamscreen:
05/31/03 16:06  smtp-proxy[143]:     2900    Message has X-Mime-Key header
05/31/03 16:06  smtp-proxy[143]:     4300    Message has X-VMP-Text header
05/31/03 16:06  smtp-proxy[143]:     2900    Message has X-PMFLAGS header
05/31/03 16:06  smtp-proxy[143]:     Score   : 10100
05/31/03 16:06  smtp-proxy[143]:     Required: 5000
05/31/03 16:06  smtp-proxy[143]:
```